Streamlining Directory Services in Georgia Government: An Enterprise Approach

Georgia Digital Academy
on Active Directory

Summer 2002

F I N A L R E P O R T

Submission Date

November 1 , 2002

Prepared for

Robert Woodruff
Director of the Technology Office
Georgia Technology Authority
Atlanta, Georgia

Prepared by

Participants of the
Georgia Digital Academy on Active Directory

Compiled and Edited by

David Craig, Georgia Technology Authority
Doris R. Konneh, Georgia Technology Authority
Richard Halstead-Nussloch, Southern Polytechnic State University

TABLE OF CONTENTS

Table 1

Participants: Georgia Digital Academy on Active Directory

Last Name	First Name	Agency	Email	Position
Bolton	Lynn	DOA *	boltonln@audits.state.ga.us	Director, IT
Brown	Alex	PAP	alexb@pap.state.ga.us	
Carter	Pam	SBWC	carterp@sbwc.state.ga.us	MIS Officer
Craig	David	GTA	dcraig@gta.ga.gov	Enterprise Sys. Architect
Crew	Willie	GTA	wcrew@gta.ga.gov	Policy and Planning
Davis	Kirby	DOA *		
Davis	Leah	DJJ	leahdavis@djj.state.ga.us	Business Analyst
Diggs	Stephen	Diggs Consulting Inc.	W4epi@amsat.org	Principal Consultant
Dixon	Beverly	CJCC	bdixon@cjcc.state.ga.us	LAN Administrator
Droutman	Erik	CCE		
Ferguson	Lisa	OTFS	lcmock@otfs.state.ga.us	Mgr., Info. Systems
Gant	Tim	TRSGA	tim.gant@trsga.com	LAN Sys. Supv.
Gibson	Kevin	GDOT	kevin.gibson@dot.state.ga.us	Sys. Adm.
Gilbert	Debra	GPB	dgilbert@gpb.org	
Gillin	Jim	MCS	jgillin@microsoft.com	
Golden	Richie	DNR	rgolden@dnr.state.ga.us	
Halstead-Nussloch	Richard	SPSU	rhalstea@spsu.edu	Facilitator
Hampton	Buster	GPB	bhampton@gpb.org	
Hannah	David	Cox Communications	David.hannah@cox.com	Mgr., Infrastructure
Head	Robbie	GTA	rhead@gta.ga.gov	Mgr., IT Help Desk
Herbert	Tim	MCS	thebert@microsoft.com	Consultant
Hunt	Daniel			
Hutsell	Elaine	DOA *	hutselle@audits.state.ga.us	Computer Auditing Specialist
Jackson	Kevin	DOC	Jacksk00@docstate.ga.us	
Johnson	Bobby	GMS	rwj@gms.state.ga.us	LAN Administrator
Kessler	Michael	DMVS	mkessler@dmvs.ga.gov	Dir., Sys. Arch.
Khalique	Mohammad	DOR	mkhaliqu@gw.rev.state.ga.us	Network Engineer
Konneh	Doris	GTA	dkonneh@gta.ga.gov	Exec Staff

Leaphart	Denise	DBF	leap@dbf.state.ga.us	Data Resource Mgr.
Lange	Mark	DCOR	langem00@dcor.state.ga.us	
Leclair	Bryan	DCA	bleclair@dca.state.ga.us	Net & Server Support Mgr
Lively	Al	DOA *	livelyal@audits.state.ga.us	IT Auditor
Lynn	Joan	DJJ	joanlynn@djj.state.ga.us	DBA/Network Mgr.
Mason	Kirk	DHR	akmason@dhr.state.ga.us	
Moore	Derrick	GMS	dmoore@gms.state.ga.us	Network Adm.
McGinn	Ed	MCS	edmcginn@microsoft.com	Consultant
McHugh-Parrish	Maggie	GoalModels	Maggie@goalmodels.com	Senior Consultant
Morgan	Micah	GTA	mmorgan@gta.ga.gov	Solutions/Sys. Engr.
Mteirek	Ghassan	MCS	ghassanm@microsoft.com	Enterprise Strategy Consultant
Samuel	Nino	PAP	ninos@pap.state.ga.gov	Asst. IT Director
Patterson	Terry	DHR	tpatterson@dhr.state.ga.us	
Pealor	Terry	DHR	tpealor@dhr.state.ga.us	
Reagan	Steve	DHR	rsreagan@dhr.state.ga.us	
Register	Jeannette	DCH	jregister@dch.state.ga.us	Network Adm.
Reynolds	Dennis	GDOT	dennis.reynolds@dot.state.ga.us	Group Leader, Ser. Ops/Support
Ruby	John	MCS	johnruby@microsoft.com	Consultant
Sailers	Michele	GBI	michele.sailers@gbi.state.ga.us	
Sanders	Eric	DHR	egsanders@dhr.state.ga.us	
Schifter	Stuart	MCS	stuarts@microsoft.com	
Sharpe	Joe	DOR	jsharpe@gw.rev.state.ga..us	Network Engr. II
Shuey	Craig	Perfect Affinity, Inc.	Craig.shuey@perfectaffinity.com	
Smith	Mike	DOA *	smithmj@audits.state.ga.us	
Thornton	Robert	CJCC	rthonto@cjcc.state.ga.us	
Thurley	Ian	GTA	ithurley@gta.ga.gov	
Tollison	Joe	DCA	jtolliso@dca.state.ga.us	Asst. Office Dir., Solutions Dev.
Tomlinson	Chris	GTA	ctomlinson@gta.ga.gov	
Wilkins	Kevin	TRSGA	kevin.wilkins@trsga.com	
Wyatt	Bill	DOA *	wyattbg@audits.state.ga.us	

*__NOTE:__ *The Department of Audits was invited to participate in the GDAAD. Its representatives viewed such participation as an opportunity to (1) interact with information technology professionals from various agencies within state government, (2) stay abreast of new information technology initiatives, (3) assist auditors in the preparation of audit materials that reflect the changing information technology environment, and (4) offer recommendations/observations/guidance in a purely advisory, non-voting role.*

1. ABSTRACT

This final report on the summer 2002 session of the Georgia Digital Academy on Active Directory (GDAAD) is submitted for review and approval by the Director of the Technology Office, his designee, and all other appropriate parties of the Georgia Technology Authority (GTA). It contains the recommended policies, standards, procedures, and guidelines for the design and implementation of active directory on an enterprise level. The report's content was developed, reviewed, and agreed upon by representatives from state of Georgia agencies who served as participants in the GDAAD.

The feedback obtained from the Director's review will be used in the formulation of the initial agendas for two organizations that resulted from the GDAAD:

- Georgia Active Directory Professional Association (GADPA), also known as a "community of practice"
- Georgia Active Directory Advisory Committee (GADAC), which will perform technical reviews of changes to active directory

Establishment of the GDAAD was motivated by two urgent movements for change in Georgia's information technology (IT) environment:

- creation of the GTA
- proposed outsourcing of information technology (IT) services statewide

First, creation of the GTA in 2000 precipitated a movement toward treating IT in an enterprise fashion and statewide standardization of IT. Although the details and processes of such standardization are still under development, the citizens of Georgia will be the ultimate beneficiaries of this effort.

Second, the movement toward outsourcing many IT services statewide is well underway with the CCOP[1] bid process. When a State or agency IT network is outsourced, the role of State personnel becomes indirect—one of manager or overseer—as opposed to direct operator. For outsourcing to be successful, opportunities must exist for the vendor and the State to reap the benefits of economies of scale, which make standardization more important.

Thus, the fundamental motivation of the GDAAD was to create coherent, well-integrated directory services that meet the needs of Georgia's citizens. Its aim: to harness and use the expertise of agency professionals to connect the "islands" of IT into an effective, efficient set of services built on active directory.

[1] CCOP –Converged Communications Outsourcing Project

2. SUMMARY

Over a period of ten weeks (July 2 - September 3, 2002), network administrators from diverse agencies (small, medium, and large) across the State worked diligently to address the issue of streamlining directory services. The primary goal of this effort was to partner with the GTA in developing and standardizing an enterprise active directory (AD) design. Such a design will be a prime factor in making it possible for the agencies to work collaboratively with the Outsource Vendor (commonly known as "CCOP") in managing the effective, efficient delivery of such services to the stakeholders of state, local, and federal governments. Three days of intensive training (June 25 – 27) were provided to bring all participants up to a minimum level of understanding of active directory.

A brief summary of the accomplishments of the GDAAD is presented in this final report:

- Development of an active directory design plan (template) for deployment by the Outsource Vendor on a state enterprise level
- Review of a set of proposed policies for active directory implementation on a statewide basis
- Review and/or formulation of a set of recommended standards, procedures, guidelines, and best practices for implementation of active directory on a statewide basis
- Establishment of the GADAC as a recommendation body to function in conjunction with the GTA and the Georgia Enterprise Information Technology Leadership Forum (GEITLF) in managing active directory services
- Development of preliminary plans for the formation and implementation of the GADA

The body of the report is organized into the following major sections:

- **Introduction** – Gives an overview of the purpose of the GDAAD, including the goals, activities, and participants.
- **Methods and Procedures** – Describes how the participants executed their functions.
- **Results and Discussion** – Presents the recommended policies, standards, procedures, guidelines, and best practices for the implementation of active directory services in Georgia.
- **Georgia Active Directory Advisory Committee** – Describes the mission, vision, goals, and objectives of this recommendation body.
- **Georgia Active Directory Professional Association** – Describes the proposed work plan, activities, deliverables, and benefits to be derived from membership in a professional association.
- **Georgia Active Directory Pilot Session –** Describes the design and implementation of the initial effort for deployment of the outcomes of the GDAAD with a select group of state agencies.

- **Conclusions** – Specifies the major findings and “lessons learned” from the GDAAD experience.
- **Recommendations** – Delineates the participants’ suggestions for how the results of the GDAAD may be used to advance the deployment of policies, standards, procedures, guidelines, and best practices for active directory on an enterprise level.
- **Next Steps** – Delineates pending items from the GDAAD that will be addressed by the GADPA, GADAC, GEITLF, or GTA. (Security is a major item.)
- **Terms and Definitions** – Contains brief explanations of key words and acronyms that were agreed upon by the GDAAD participants.
- **Appendices** – Contains the major source materials used in the GDAAD.

3. INTRODUCTION

A major challenge of the 21st century is how to make Georgia state government more responsive to the needs of its citizens. One of the primary ways to meet this challenge is the effective, efficient use of IT resources.

An approach that has yielded substantial benefits in other states, most notably Washington, is the fostering of relationships among government agencies by providing a means for them to come together to solve common problems. Thus, rather than being concerned for their *individual needs only*, agencies are beginning to view each other as partners in the ever-changing world of IT and are, as a result, becoming advocates for cultural change.

The Georgia Digital Academy (GDA) is an example of the movement toward collaboration among state government agencies. It serves as a prime catalyst for agencies to come together to develop solutions to common technical and business problems.

3.1 Goals and Activities of the Georgia Digital Academy on Active Directory

For its second session, the GDA undertook the problem of how to design and prepare for the statewide adoption of Microsoft™ Active Directory.[2] Active Directory is one of the directory services products that Georgia will use in collaboration with the Outsource Vendor for streamlining information technology resources on an enterprise basis. As used in the GDA and on a statewide level, it is defined as follows:

> ***Active Directory*** *- The published standard for Network Directory for the State of Georgia.*

Under the leadership of GTA's Technology Office, the GDAAD was conducted at Southern Polytechnic State University (SPSU). It consisted of:

- An initial ("kickoff") Active Directory technical session, which provided a common base of knowledge for participants by compressing information from two Microsoft courses (8 days) into three days (June 25 – 27).

- Ten weeks of facilitated learning sessions each Tuesday (July 2 - September 3), which were structured around an ongoing group activity—the planning, designing, and standardizing of active directory statewide.

[2] The first session of the Georgia Digital Academy focused on the issue of document management technology. See the GTA website at www.gagta.com for a copy of the final report.

- Nine weeks of optional half-day consultative sessions each Wednesday following Tuesday's full-day session. Participants requested additional explanations and supplemental briefings, as needed, and refined work products, as appropriate, to meet the GDAAD's overall needs.

Currently, no State policies, standards, procedures, or guidelines exist for how to efficiently and effectively implement and manage directory services across the statewide enterprise. This GDAAD aimed to bring together the multiplicity of existing individual networks and domains into a coherent, integrated, manageable structure under the umbrella of AD.

3.1.1 Goals

The specific goals of the GDAAD were to:

- facilitate collaboration and education among state entities,
- accelerate the identification and standardization of best practices throughout the state enterprise,
- incubate solutions to meet the business requirements of state entities, and
- manage the relationship between the State and the Outsource Vendor.

3.1.2 Activities

The specific activities in which the GDAAD engaged to accomplish its goals included:

- learning the active directory technology;
- defining, examining and refining policies, standards, and procedures pertinent to implementing active directory across state government;
- identifying how active directory technology can enable agencies to manage directories and directory services more easily and efficiently;
- developing techniques and protocols through active directory for working with and managing the Outsource Vendor; and
- planning the design of active directory to be implemented by State agencies.

3.2 Resources of the Georgia Digital Academy on Active Directory

To achieve the goals of the GDAAD, a variety of resources were employed. These resources are broadly classified as *human*, *training materials*, and *information*.

3.2.1 Human Resources

The GDAAD relied on professionals who possess expertise in a variety of areas:

- Facilitators, trainers, and SMEs[3] from SPSU
- GTA liaison representatives
- Office of Planning and Budget representative
- SME consultants from both industry and Microsoft

The following presentations by the SMEs ranged from the proposed Outsource Vendor's role in AD to how to conduct audits:

- AD in CCOP Overview
- Auditing against Standards
- Budget Implications for AD in CCOP
- GTA Assumptions on Roles/GDAAD Deliverables

3.2.2 Training Materials Resources

The following Microsoft training materials were used in the AD technical session:

- Designing a Microsoft Windows 2000 Directory Services Infrastructure (Course 1561)
- Implementing and Administering Microsoft Windows 2000 Directory Services (Course 2154)

3.2.3 Information Resources

From the outset, the participants voted unanimously to conduct some of the GDAAD activities electronically. To function effectively in this online community, the following information resources were mobilized:

- A comprehensive CD-ROM of all pertinent input information:[4]
  - GTA policies, standards, and procedures
  - Request for proposal (RFP) for the Outsource Vendor (CCOP)
  - GDAAD schedule and exercises
  - Presentations
- A listserve for communication of work items
- A secure website for displaying work outputs

[3] SME – Subject Matter Expert
[4] This input information was distributed on June 27, 2002.

4. METHODS AND PROCEDURES

The GDAAD employed multiple methods and procedures for group problem solving; formulation of recommended policies, standards, guidelines, and best practices; construction of proposals; and research. Specific approaches included:

- ***Brainstorming*** - Identifying ideas rapidly; e.g., to quickly develop lists of required elements in AD procedures.
- ***Computer-Mediated Problem Solving*** - Utilizing a listserve and web site by which participants were able to continue to work collaboratively throughout the week.
- ***Divide and Conquer*** - Decomposing a large issue into areas and assigning a subgroup to work on them; e.g., the division of AD security into four major areas.
- ***Group Heuristic Development and Improvement*** - Utilizing the professional expert judgment within the whole group or a subgroup to formulate appropriate new solutions or improve existing solutions in AD structuring and standardization. For example, the Wednesday subgroup provided the details and rationale for the GADAC standard that was adopted by the whole GDAAD.
- ***Group Heuristic Evaluation*** - Utilizing the professional expert judgment within a group or subgroup (which might or might not be guided by identified criteria) to evaluate the appropriateness of standards, guidelines, and best practices for meeting the directory services needs of the participating agencies and the State. For example, both the subgroups and the whole GDAAD examined the four policies for their applicability to AD.
- ***Research*** - Utilizing repositories, web sites of pertinent industry and professional organizations, and publications to access pertinent AD and directory services issues and solutions; e.g., *Microsoft White Papers and Best Practices* that may be appropriate for the State.

The intent of using these approaches was to obtain AD standardization and best practices as of a particular point in time (June - September of 2002). In the spirit of continuous improvement, the results of the subgroups should be reexamined, as necessary, to continually update them.

5. RESULTS AND DISCUSSION

To ensure the successful implementation of active directory on an enterprise level, an understanding and delineation of the components for which state agencies and the Outsource Vendor will be responsible is critical. A concise summary of those components and responsibilities follows:

Root Domain and Master

The GTA staff will maintain and operate the root domain controllers by performing the following root master roles:

- Domain Naming Master
- Infrastructure Master
- Primary Domain Controller Emulator (if necessary)
- Root RID Master
- Schema Master

LAN Administration

The Outsource Vendor will be responsible for all LAN Administration, including but not limited to:

- Desktop support
- DNS (below the root level)
- Exchange servers
- File and print servers maintenance
- User Accounts
- Vendor Domain

The output from the GDAAD will be used to govern how the Outsource Vendor and the agencies implement and maintain these components. That is, the Outsource Vendor and the agencies must abide by the participants' recommended policies, standards, procedures, guidelines, and best practices.

While the Outsource Vendor has a vested interest in simplicity and uniformity of the active directory design, participants in the GDAAD wanted to ensure that such a design would allow maximum flexibility to accommodate the diversity of State agencies' operations. Therefore, in addressing the various components of active directory, the participants considered such areas as:

- Enterprise requirements
- Complexity of individual agencies' business needs
- Allowances for individual agencies' management styles

5.1 Recommended Enterprise Policies

This section contains the following recommended policies for active directory design and implementation that were generated by the GDAAD:

- Forest Policy
- Domain Policy
- Organizational Unit Policy
- Site Policy

Forest Policy

Topical Area: AD Policies	Standard Number:
Effective Date:	Revision Date: 10/1/2002

AUTHORITY

The Georgia Technology Authority (GTA) establishes policies for technology architecture and has the authority to create policies, standards, procedures, and guidelines for all business units and computer assets that operate on the State's enterprise network backbone.

SCOPE

This policy applies to all State owned and managed resources and software that are connected to the State's active directory topology. This policy covers implementation of any active directory Forest established on the State's enterprise network within a production environment.

PURPOSE

To define an effective, scalable, secure and manageable active directory Forest design and to facilitate one standardized infrastructure for the State's active directory, which will reduce multiple sign-ons and total cost of ownership for the State's network operations.

DEFINITIONS

- Georgia Active Directory Advisory Committee (GADAC) – A body that represents all state agencies in making recommendations on matters affecting active directory. This group reports to the Georgia Enterprise Information Technology Leadership Forum (GEITLF).

- Georgia Enterprise Information Technology Leadership Forum (GEITLF) - A body that represents the IT leadership of the agencies and is empowered to make recommendations to GTA.

1. FOREST PLAN

There is one enterprise forest structure for the State of Georgia, with justified exceptions.

The GTA is responsible for the availability of the State Forest infrastructure enabled for active directory services and will retain control of the Forest Root

Domain, in coordination with the GADAC. The GTA will be responsible for maintaining AD services to ensure business continuity for each agency.

2. SCHEMA CONTROL AND SECURITY

Requests for enterprise Schema modifications and security policy changes must be approved by the GTA, as recommended by the GADAC.

Membership in the Root Domain Schema, Enterprise and Domain Admin groups is restricted and controlled by the GTA, as recommended by the GADAC.

The GTA will ensure that only properly authorized changes are implemented, as reviewed by the GADAC.

3. EXCEPTION POLICY

Agencies who have a business case for an exception to the one enterprise forest plan must submit a forest design exception request to the GTA, in accordance with the current State standards and procedures. The request will be forwarded to the GADAC for technical evaluation and recommendation to the GEITLF. The GEITLF will then make a recommendation to GTA.

All Forests established within the State's enterprise network infrastructure will be owned and managed by the GTA, in coordination with the GADAC, unless expressly stipulated and agreed to in the exception request.

4. BACKUP AND DISASTER RECOVERY

Backup and recovery of the forest root domain will be the sole responsibility of GTA.

5. ACTIVE DIRECTORY REPLICATION

Replication of the enterprise forest root domain will be the responsibility of GTA.

Domain Policy

Topical Area: AD Policies	Standard Number:
Effective Date:	Revision Date: 10/1/2002

AUTHORITY

The Georgia Technology Authority (GTA) establishes policies for technology architecture and has the authority to create policies, standards, procedures, and guidelines for all business units and computer assets that operate on the State's enterprise network backbone.

SCOPE

This policy applies to all State owned and managed resources and software that are connected to the State's active directory topology. This policy covers implementation of any active directory Domain within the State owned domain, established on the State's enterprise network.

PURPOSE

To define an effective, scalable, secure and manageable active directory Domain design and to facilitate one standardized infrastructure for the State's active directory, which will reduce multiple sign-ons and total cost of ownership for the State's network operations.

1. DOMAIN PLAN

There will be a single, dedicated root domain for any/all forests. This will provide a controlled environment for forest wide change management and limit the amount of replicated data. The root domain will contain no user accounts and will be used strictly as an empty domain to manage the schema, global catalog, site topology, security and enterprise policy.

The GTA will be responsible for the operation of the enterprise forest root domain, in coordination with the Georgia Active Directory Advisory Committee (GADAC). The GTA is also responsible for the replication, redundancy and backup of the enterprise domain.

Each agency shall have the option of its own domain under the enterprise forest root domain. Based on business requirements and upon recommendation of the GADAC, agency sub-domains may be created.

All domains established beneath the State's enterprise domain will be owned by the agencies, and they will oversee management of their domains. Oversight

management will be implemented in accordance with current State standards. These domains will be established within the forest as defined in the Forest policy.

2. DOMAIN CONTROL AND SECURITY

Membership in the dedicated enterprise forest root domain Schema, Enterprise and Domain Admin groups is restricted and controlled by the GADAC and implemented by the GTA.

The GTA will maintain a high level of security on all levels to ensure that only properly authorized changes are implemented.

3. BACKUP AND DISASTER RECOVERY

Backup and recovery of the dedicated enterprise forest root domain will be the responsibility of the GTA.

4. ACTIVE DIRECTORY REPLICATION

Replication of the enterprise forest root domain will be the responsibility of GTA.

1. DOMAIN NAME SERVICES ZONES

The primary Domain Name Services (DNS) zone for the State of Georgia is owned and managed by the Georgia Technology Authority. DNS support for active directory for the State appears as a sub zone and is replicated between all DNS servers in the dedicated enterprise forest root domain.

Agencies may create and manage sub-zones to the active directory zone in accordance with current State standards. All DNS zones used by active directory will be implemented as active directory integrated zones.

Organizational Unit Policy

Topical Area: AD Policies	Standard Number:
Effective Date:	Revision Date: 10/1/2002

AUTHORITY

The Georgia Technology Authority (GTA) establishes policies for technology architecture and has the authority to create policies, standards, procedures, and guidelines for all business units and computer assets that operate on the State's enterprise network backbone within the State of Georgia.

SCOPE

This policy applies to all State owned and managed resources and software that are connected to the State's active directory topology. This policy covers implementation of any active directory Organizational Unit (OU) within the State owned domain, established on the State's enterprise network.

PURPOSE

To define an effective, scalable, secure and manageable active directory OU design and to facilitate one standardized infrastructure for the State's active directory, which will reduce multiple sign-ons and total cost of ownership for the State's network operations.

1. OU PLAN

Each Agency manages its objects in the directory while the GTA, in coordination with the Georgia Active Directory Advisory Committee (GADAC), manages the configuration of the directory service.

The domain owner (the agency) is responsible for completing an initial OU design for the domain and for submitting it to the GTA. The design will be forwarded to the GADAC for technical evaluation and recommendation to the Georgia Enterprise Information Technology Leadership Forum (GEITLF).

2. OU CONTROL

The domain owner is responsible for the management of all OUs and submission of requests for creation of all OUs under its domain(s).

3. OU OWNERSHIP

The domain owner designates an owner for each OU. Each OU owner is a data manager with control over a sub-tree of objects in active directory.

OU owners do not own or control the operation of the service; it remains under the control of the domain owner.

Site Policy

Topical Area: AD Policies	Standard Number:
Effective Date:	Revision Date: 10/1/2002

AUTHORITY

The Georgia Technology Authority (GTA) establishes policies for technology architecture and has the authority to create policies, standards, procedures, and guidelines for all business units and computer assets that operate on the State's enterprise network backbone.

SCOPE

This policy applies to all State owned and managed resources and software that are connected to the State's active directory topology. This policy covers implementation of any active directory site within the State owned domain, established on the State's enterprise network.

PURPOSE

To define an effective, scalable, secure and manageable active directory Site design and to facilitate one standardized infrastructure for the State's active directory, which will reduce multiple sign-ons and total cost of ownership for the State's network operations.

1. SITE PLAN

This policy defines an active directory Site as a set of well-connected IP subnets, equivalent to LAN speeds or greater.

In conjunction with the GTA and the Outsource Vendor, sites are to be designed by the Agency(ies) affected. The Agency's primary objective is to design a site topology that reduces WAN utilization during active directory replication and client logon.

The Agency is responsible for the submission of the site topology design to the GTA. The design will be forwarded to the Georgia Active Directory Advisory Committee (GADAC) for technical evaluation and recommendation to the Georgia Enterprise Information Technology Leadership Forum (GEITLF). The GEITLF will then make a recommendation to the GTA.

2. SITE CONTROL

The Agency understands the conditions of the network between that Agency's sites.

Site Policy

Topical Area: AD Policies	Standard Number:
Effective Date:	Revision Date: 10/1/2002

In addition to liaison with the GTA, the Agency's responsibilities include providing advice and consent on:

- Changes to site topology
- Location of domain controllers

5.2 Recommended Enterprise Standards and Procedures

This section of the final report contains the following recommended standards and procedures for active directory design and implementation that were generated by the GDAAD:

- Georgia Active Directory Advisory Committee
- Account Management
- Active Directory Structure
- Auditability
- Availability
- Change Management
- Disaster Recovery
- DNS Maintenance
- Domain Maintenance
- Exemption Request
- Naming Standard
- Organizational Unit Standard
- Password Reset Standard
- Review Cycle
- Schema Change Procedure
- Security
- Site Maintenance

Georgia Active Directory Advisory Committee

The Georgia Active Directory Advisory Committee (GADAC) is one of three entities that were created during the Georgia Digital Academy on Active Directory. [5] The goal was to create a group with representatives from various state agencies to serve in an advisory capacity to GTA and GEITLF on active directory related issues. As such, a standard was developed for its organization and operation.

The GADAC will work to maintain an effective framework of AD policies and standards and review proposed changes to the AD structure. It will also provide an avenue via the GTA for individual agencies to request exceptions and file grievances and, generally, provide feedback on the AD process.

Details about the GADAC Standard are found in the following section.

[5] The other two entities were the Georgia Active Directory Professional Association and the Georgia Active Directory Pilot Project. See Sections 6 and 7 of this final report for details.

Georgia Active Directory Advisory Committee

Topical Area: Active Directory Governance	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To establish the Georgia Active Directory Advisory Committee (GADAC) and further define the activities assigned to it in the Georgia enterprise active directory policies.

2. SCOPE

Recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

3. DEFINITIONS

3.1 Active Directory Policies, Standards and Procedures - Forest, Domain, Organizational Unit, and Site Policies, including all supporting standards and procedures

3.2 Active Directory Operations - Policy exceptions, schema modifications, agency sub-domains, OU naming, and AD administrator selection criteria

4. STANDARD

4.1 GADAC Organization

4.1.1 Membership

GADAC membership consists of:

- 14 members
- 1 GTA representative
- 1 GEITLF representative (advisory and non-voting)
- 1 DOA representative (advisory and non-voting)
- 1 GADPA representative (advisory and non-voting)

Topical Area: Active Directory Governance	Standard Number:
Effective Date:	Revision Date: 10/1/2002

4.1.2 Representation

Initial membership of the GADAC comes from the GDAAD participating agencies. Member representatives must have a practical knowledge of active directory technology. Appointment as a Representative is for a two-year period, staggered such that 50 percent of the membership rotates every year. The nine largest non-constitutional state agencies (as measured by employee count) will have permanent voting membership, while the remaining seats will rotate among all other agencies on a voluntary lottery basis. Participating agencies need to be represented at 75 percent of GADAC meetings per year to maintain voting status.

4.1.3 Communication

Notification of Committee action will be made to all agencies via open email list service. Only GADAC members can post. Each Agency will maintain at least two addresses in the list membership.

Minutes will be taken at all meetings.

A Web-based secure service will be used to support threaded discussions, document storage, and other committee functions. Members will have read/write access. Non-members will have read only access. There will be a secure area where sensitive information can be kept that will be accessible by members only.

The address for the GADAC website is http://ad-sharepoint.gagta.com.

4.1.4 Operations

Committee action is taken by majority rule of voting members present by a show of hands.

For emergencies, votes can be taken via electronic means.

There must be at least 8 votes cast to make a decision.

Meetings will occur at least once every thirty days on a date prior to the monthly GEITLF meeting. Requests for recommendations can be tabled for one meeting cycle only.

A Chairperson will be elected by the GADAC from its membership, and will be responsible for:

- Committee record-keeping and distribution
- Maintenance and distribution of members' contact information
- Meeting agenda and conduct
- Maintenance of attendance records
- Facilitation of all GADAC meetings and activities

Observers can attend meetings but cannot participate in discussions. Non-members can send a request to the GADAC chairperson requesting to address the GADAC.

4.2 Active Directory Policies, Standards, and Procedures

The Committee will make recommendations for changes and additions to active directory policies, standards, and procedures as necessary.

4.3 Active Directory Operations

- The GADAC will coordinate with the GTA on matters affecting active directory operations and availability of the state forest root domain, and configuration of the directory service.

- The GADAC will make recommendations on the membership of the root domain Schema, Enterprise, and all domain administrators groups.

- The GADAC will review proposed Schema changes received by the GTA.

- The GADAC will review operational procedures at the request of the Outsource Vendor (CCOP) Service Committee, GTA or the GADAC voting membership.

- The GADAC will evaluate proposals for exceptions to the AD forest policy and make recommendations to the GEITLF group

- The GADAC will evaluate proposals for agency sub-domains and make recommendations to the GTA.

- The GADAC will evaluate proposals for agency OU designs, and make recommendations to the GTA.

- The GADAC will evaluate proposals for agency Site topology designs and make recommendations to the GTA.

- The GADAC may request the initiation of policy compliance reviews within its scope.

4.4 GADAC Operations Review

The GADAC will review and amend this standards document as necessary to maintain the effectiveness of the Committee. This review will also include verification of voting membership status and any such status actions as are deemed necessary to maintain attendance.

5. REFERENCES

- Exemption Request
- Review Cycle

6. REVIEW SCHEDULE

This standard will be reviewed annually.

Account Management

Topical Area: Account Management	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to add, change, or delete an account in the active directory for the State of Georgia. Account Management also includes changing access rights to resources for accounts.

2. SCOPE

All state employees and others who are given an account in active directory for the State of Georgia.

3. RATIONALE

The duties for governing accounts are divided between two roles:

- Agencies control their employees and other accounts for vendor-supported servers through instructions to the Outsource Vendor (per existing policy). They also implement changes to accounts for out-of-scope servers.
- Outsource Vendor implements changes to accounts requested by agencies.

A procedure must be implemented to allow effective interaction between the roles of agencies and the Outsource Vendor.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – The organization that supports the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4.3 Agency-managed – Active directory components that are directly administered by agencies.

4.4 Outsource Vendor-managed – Active directory components that are administered by the Outsource Vendor. Originally chartered in the CCOP Contract (2003).

4.5 E-form – A secure electronic medium for transmitting requests to the Outsource Vendor.

4.6 Authorized Agency Managers – Agency staff that have been designated by their agency and identified to the Outsource Vendor to authorize active directory functions.

4.7 Agency IT Support – An agency representative who handles requests for agency-managed servers and communicates changes to agency users.

5. RESPONSIBILITIES

Agency	Completes E-forms to specify all changes to user accounts that involve Outsource Vendor-managed servers.
Outsource Vendor	o Implements changes to accounts per agency requests.
Agency IT Support	o Implements changes to accounts for granting access to agency-managed resources. o Relays changes to accounts to users.

6. PROCEDURE

6.1 Add or Change Account

RESPONSIBILITY	STEP
Agency	1. Completes agency business process for creating/changing accounts.
Authorized Agency Manager	2. Completes E-form signed by authorized agency contact(s) to Outsource Vendor.
Outsource Vendor	3. Creates/changes user account. 4. Creates/changes email account. 5. Creates/changes permissions on Outsource Vendor-managed servers. 6. Creates/changes group memberships
Agency IT Support	7. Adds/changes permissions on Agency-managed servers, as needed. 8. Notifies employee and supervisor, closes ticket.

Topical Area: Account Management	Standard Number:
Effective Date:	Revision Date: 10/1/2002

6.2 Delete Account

Agency	1. Completes agency business process for deleting an account.
Authorized Agency Manager	2. Fills out E-form to delete an account.
Outsource Vendor	3. Deletes Home Drive after 90 days. (Agency can request an extension.)
	4. - Disables and hides email account for 90 days; then deletes. (Agency can request an extension.) - Creates a standard auto-reply message when account is disabled. (Agency can customize auto-reply message on a case-by- case basis.)

6.3 Agency-to-Agency Transfer

An Agency-to-Agency Transfer should be handled in the same fashion as a **delete** from the loosing agency and a **new hire** from the gaining agency.

6.4 Expedited Account Deletion

Authorized Agency Manager	1. Fills out E-form marked as 'expedite' to delete an account.
Outsource Vendor	2. Performs steps 3 and 4 of the normal **Delete** process.
Outsource Vendor	3. Completes all changes within a maximum of 15 minutes at the local level and 180 minutes statewide.

6.5 Emergency Account Deletion

Authorized Agency Manager	1. Contacts Outsource Vendor using password reset authentication mechanism and requests emergency account deletion. The agency completes an E-form after the fact to provide an audit trail. (Agency determines if this is an emergency deletion.)
Outsource Vendor	2. Disables account according to the **Disable Account** process within 15 minutes at the AD site in which the account is located.
Outsource Vendor	3. Maintains replication mechanism that updates AD in entire system within 3 hours.
Outsource Vendor	4. Disables email account and Home Drive per steps 3 and 4 of the normal **Delete Account** process.

7. EXCEPTIONS

No exception policies as of this revision date.

8. REFERENCES

- Review Cycle
- Security Policies

- A process for disabling a telephone that coincides with the **Account Deletion** process should also be implemented.
- An agency-driven pick list on E-form, rather than a free-form field, should insure reporting. Different applications appear in the pick list for different agencies.
- An incident number will be provided for each received E-form.
- A Web interface to view incident status, along with the E-form, will be provided.
- E-form will contain Originator contact information, an appropriate authorized electronic signature, account identification information and permissions and groups (as needed). The Outsource Vendor will retain all

e-forms for a minimum of one year or to meet the Agency's retention requirements, if longer.

Active Directory Structure

Topical Area: Active Directory Structure	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To communicate standards for implementation of the statewide active directory structure. The standard represents Georgia active directory policies, without reference to approved exceptions.

2. SCOPE

All outsourcing vendors and state agencies.

3. DEFINITIONS

3.1 **Agency Domain Administrator** – A user account that is a member of the domain administrators global group in a domain created to house out-of-scope computer assets.

3.2 **Agency-supported** - Database servers, application servers, web servers, and resource management servers.

3.3 **Domain** – An active directory security boundary.

3.4 **Forest** – A group of active directory domains that trust each other.

3.5 **Forest Root** – The first domain created in the Georgia active directory implementation.

3.6 **Organizational Unit** – An active directory administrative boundary.

3.7 **Root Domain Administrator –** A user account that is a member of the domain administrators global group, enterprise administrators global group, or schema administrators global group in the active directory forest root domain.

3.8 **Site** – A location in active directory that is one or more well-connected TCP/IP subnets.

3.9 **Vendor Domain Administrator –** A user account assigned to an Outsource Vendor employee that is a member of a domain administrators global group.

3.10 Vendor-supported - Computing assets defined as *in scope* (see Section 6.7.6 of the CCOP Contract), plus printers, workstations, and all associated functions.

4. Structure

The initial design takes advantage of the flexibility of domains and organizational units (OUs) in active directory. An empty forest root was utilized to maximize security of the forest root; allow child domains to be reorganized, as necessary; and recognize the differing roles among the GTA, state agencies, and the Outsource Vendor.

- A single forest design was employed to reduce total costs, create a single Exchange 2000 organization, and ease administration.

- A single accounts domain was utilized to create a simple administrative structure for the Outsource Vendor. Resource domains were used to separate administration of systems maintained by their respective agencies.

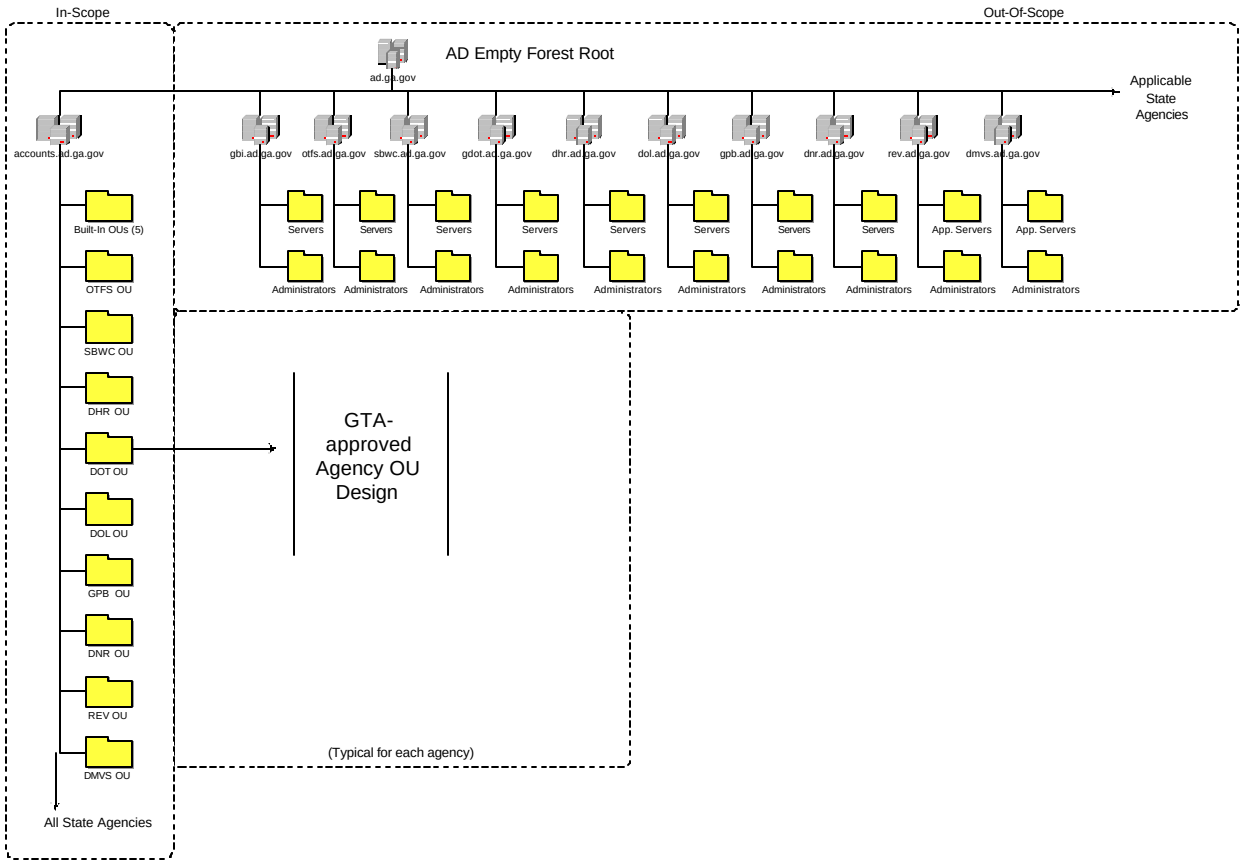
- Top-level OUs were created for each state agency in the accounts domain to allow for the application of separate group policy objects.

- All OU designs are governed by the State OU Design Standard and must be approved by the GTA.

Active Directory Structure

Topical Area: Active Directory Structure	Standard Number:
Effective Date:	Revision Date: 10/1/2002

5. Drawing



6. REFERENCES

- Review Cycle
- Exemption Request
- Forest, Domain, OU and Site Policies

Auditability

Topical Area: Auditability	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To ensure that all servers and software complies with applicable procedures and standards.

2. SCOPE

All servers participating in active directory, whether managed by GTA, the Outsource Vendor, or agencies.

3. DEFINITIONS

3.1 Outsource Vendor – Vendor charged with supporting the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4. STANDARD

4.1 Log Files

- Logs must be maintained for a minimum of 6 months.
- Logs will be available to internal auditors.
- Exception reports from the logs will be reviewed daily and a report of summary of exceptions will be available to designated agency representatives.
- Logs must be replicated hourly to another location that is accessible only by executive-level security personnel.
- Logs should be renamed during the replication process to prevent overwriting in the replicated location.
- Log size should be set according to need, so that events within the last 60 days are easily accessible from the primary log file.

4.2 Reporting

The Outsource Vendor will:

- Provide a list of *resources against current user access levels* at least once a year and on demand by the agencies.
- Respond to log file inquiry requests within 2 business days.
- Provide weekly reports of failed login attempts to agency designee.
- Notify agency immediately of repeated failed attempts.

4.3 Events to be Logged

- Success and Failure Auditing for Logins at the root forest level and/or where all user accounts are located
- Success and Failure Auditing for Object Access at the domain level
- All user account changes (e.g., passwords)
- Schema modifications

4.4 Auditors

- There will be internal auditors.
- Agencies and auditors will have *view only* privileges for OUs in the accounts domain.

5. REFERENCES

- Review Cycle
- Security Policies

Availability

Topical Area: Availability	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To ensure that the state's active directory implementation is readily available.

2. SCOPE

All servers participating in active directory, whether managed by GTA, the Outsource Vendor, or agencies.

3. DEFINITIONS

3.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4. STANDARD

4.1 Redundancy

There will be at least three domain controllers for the root forest directory.

4.2 Backups

- One copy of a full backup of the forest root will be made daily. (Note: AD backup must be enabled at the forest root.)
- One copy of the tape will be retained for 35 days at an offsite location.
- The tape expires after 45 days,
- Tape access is limited to authorized personnel.

4.3 Disaster Recovery

An approved disaster recovery plan must be in place:

- The plan should include "mission critical" agencies and the GADAC, at a minimum.

- The plan should include scenarios for:
  - No equipment
  - No equipment and no people
  - No access to equipment

- The plan must be tested at least once a year, without prior notice to the recovery team.

- The plan must include a specified offsite location that meets industry standards for disaster recovery.

4.4 Reporting

An overall summary report of AD status (including backup status) must be available by authorized personnel for viewing at any time. Also, full detailed report must be available upon request.

5. REFERENCES

- Forest Policy
- Review Cycle
- Security Policies

Change Management

Topical Area: Change Management	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to request a change in active directory for the State of Georgia.

2. SCOPE

All changes relating to active directory for the State of Georgia.

3. RATIONALE

Given the constant change in technology and organization, a timely and formalized method of introducing change into active directory must be implemented.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GETILF and/or GTA for Active Directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – The organization that supports the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4.3 GTA Operations – The Information Resource Management branch of GTA that manages the active directory root domain.

4.4 Georgia Enterprise Information Technology Leadership Forum (GEITLF) – An advisory committee comprised of high-level IT staff from select agencies that advise on enterprise IT issues.

5. RESPONSIBILITIES

GADAC	• Performs a technical review of all change requests and makes recommendations to GTA through GEITLF.
GEITLF	• Reviews recommendations made by GADAC and submits to GTA.

Outsource Vendor	• Formulates and implements requests for changes.
Agency	• Formulates requests for changes.
GTA	• Forwards proposed changes to GADAC.
GADAC Chairperson	• Ensures that communication on proposed active directory policy, standard, and/or procedure changes are sent out via the listserve to all current GADAC members.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, Outsource Vendor, or GTA	1. Initiates a request to change some aspect of active directory by sending the request to GTA.
GTA	2. Assigns a tracking number and forwards the request to GADAC for review.
GADAC	3. Reviews the request and prepares a formal recommendation to be submitted to GTA for reconsideration within 60 days.
GTA	4. Reviews and approves/disapproves the recommendation; notifies the originator of the request.
Outsource Vendor and/or GTA Operations	5. Assigns resources. 6. Develops a schedule for testing, implementation, and a back out strategy. 7. Notifies originator and all agencies of the schedule date. 8. Implements the change. 9. Requests will be retained by the Outsource Vendor for a minimum of 1year.

7. EXCEPTIONS

No exceptions as of this revision date.

Topical Area: Change Management	Standard Number:
Effective Date:	Revision Date: 10/1/2002

8. REFERENCES

- GADAC Standard
- Review Cycle
- Security Policies

9. REQUIRED INFORMATION

The request from the Agency must include, but not be limited to, the following detailed information:

- Description of change
- Justification based on business need
- Timeframe necessary for completion or implementation
- Actions taken by GTA or the Outsource Vendor
- Contact information
- Authorized signature
- Scope
- Cost (if any)

DNS Maintenance

Topical Area: DNS Maintenance	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to make a change in the Domain Name Services (DNS) for the State of Georgia.

2. SCOPE

All changes to the DNS structure used and maintained via the active directory structure for the State of Georgia.

3. RATIONALE

The Outsource Vendor will perform the majority of DNS adds, modifications, and deletions to implement changes requested by agencies. The agencies will be responsible for replicating changes to the appropriate servers.

A procedure is required to ensure that desired changes are requested, implemented, and tracked in an effective manner.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – The organization that supports the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4.3 GTA Operations – The Information Resource Management branch of GTA that manages the active directory root domain.

4.4 GADAC Chairperson – The elected leader of the GADAC.

DNS Maintenance

Topical Area: DNS Maintenance	Standard Number:
Effective Date:	Revision Date: 10/1/2002

5. RESPONSIBILITIES

GTA Operations	• Maintains the parent DNS structure to which the active directory integrated zones connect.
GADAC	• Performs a technical review of all change requests and makes recommendations to GTA through GEITLF.
Outsource Vendor	• Performs approved changes in coordination with GTA operations.
Agency	• Formulates requests for changes.
GTA	• Reviews recommendations from GADAC and GEITLF.
GADAC Chairperson	• Handles status of change requests.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, GTA, or Outsource Vendor	1. Submits a request to change DNS to GTA.
GTA	2. Assigns a tracking number and forwards the request to GADAC.
GADAC	3. Reviews the request and prepares a formal recommendation to be submitted to GTA for reconsideration within 60 days.
GTA	4. Provides a response regarding the status of the request to the GADAC and to the originator.
	5. Instructs the Outsource Vendor and/or GTA Operations to make the change.
Outsource Vendor and/or GTA Operations	6. Assigns resources; develops a schedule
GTA	7. Approves the suggested schedule.
Outsource Vendor and/or GTA Operations	8. Performs requested action, if approved, within schedule.
GTA	9. Checks with request originator to ensure that the change met the identified needs.

10. Requests will be retained by the Outsource Vendor for a minimum of 1 year.

7. EXCEPTIONS

No exceptions as of this revision date.

8. REFERENCES

- Review Cycle
- Exemption Request
- Domain Policy
- GADAC Standard

8.1 Information to be Included

As much detail as possible should be included in each request. The following items must be included at a minimum:

- Description of add/change/delete
- Justification based on business need
- Necessary timeframe for completion or implementation
- Contact information for the request originator
- Scope of change
- Any prerequisites or coordination requirements
- Agency authorizing party signature or indication of approval

Disaster Recovery

Topical Area: Disaster Recovery	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed for **disaster recovery** in situations where active directory for the State of Georgia is impacted.

2. SCOPE

All components of active directory for the State of Georgia.

3. RATIONALE

Because active directory serves as the locator and access control for LAN-based resources, an effective plan to recover the service in case of a disaster must be implemented.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for Active Directory policies and operations within the Georgia enterprise computing environment.

4.2 Georgia Enterprise Information Technology Leadership Forum (GEITLF) - An advisory committee comprised of high-level IT staff from select agencies that advise on enterprise IT issues.

4.3 Outsource Vendor – Vendor charged with supporting the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4.4 GTA Operations – The Information Resource Management branch of GTA that manages the active directory root domain.

5. RESPONSIBILITIES

GTA Operations	• Fulfills requirements as specified in the disaster recovery plan. • Performs annual periodic tests of recovery plan. Results of the tests will be retained for at least one year.
GADAC	• Performs a technical review of the disaster

	recovery plan and makes recommendations to GTA through the GEITLF.
GEITLF	• Reviews recommendations made by GADAC and submits to GTA.
Outsource Vendor	• Fulfills role as specified in the disaster recovery plan.
Agency	• Fulfills role as specified in the disaster recovery plan.
GTA	• Proposes changes to the disaster recovery plan. • Reviews recommendations from GADAC and GEITLF.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, Outsource Vendor, or GTA	1. Determines that a disaster has occurred.
Discoverer (s) of the disaster	2. Notifies persons responsible for recovery of the affected service(s), as per the disaster recovery plan.
Agency	3. Initiates the agency's Business Continuity Plan.
Agency, Outsource Vendor, or GTA	4. Activates the designated hot site, as needed, depending on the affected components.
Agency, Outsource Vendor, or GTA	5. Disseminates public information.
Agency, Outsource Vendor, and GTA	6. Provide support services to aid recovery.

7. EXCEPTIONS

No exceptions as of this revision date.

Topical Area: Disaster Recovery	Standard Number:
Effective Date:	Revision Date: 10/1/2002

8. REFERENCES

- Review Cycle
- Security Policies

9. REQUIRED INFORMATION

The disaster recovery plan must include the following:

- Frequency of backup and offsite storage of data, applications, and the operating system
- Redundancy of critical system components or capabilities
- Documentation of system configurations and requirements
- Copy of the disaster recovery plan (which must be kept at recovery sites)

Domain Maintenance

Topical Area: GADAC	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to make a change in the active directory domain structure for the State of Georgia.

2. SCOPE

All changes to the active directory domain structure for the State of Georgia.

3. RATIONALE

The duties that govern changes to domains are divided among four roles:

- Agencies - Control their domain per existing policy.
- Outsource Vendor - Controls the domain that contains computers and users.
- GTA - Controls all actions at the root level of active directory that include domain maintenance.
- GADAC - Performs a technical review of domain maintenance requests and makes recommendations on how to proceed.

A procedure must be implemented to allow effective interaction among the four roles.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – The organization that supports the majority of active directory work. Originally chartered in the CCOP Contract (2003).

4.3 GTA Operations – The Information Resource Management branch of GTA that manages the active directory root domain.

Topical Area: GADAC	Standard Number:
Effective Date:	Revision Date: 10/1/2002

4.4 Georgia Enterprise Information Technology Leadership Forum (GEITLF) - An advisory committee comprised of high-level IT staff from select agencies that advise on enterprise IT issues.

5. RESPONSIBILITIES

GTA Operations	• Implements domain changes per the approved recommendations of the GADAC.
GADAC	• Performs a technical review of all requests and makes recommendations to GTA through GEITLF.
GEITLF	• Reviews recommendations of the GADAC and submits them to GTA.
Outsource Vendor	• Performs approved domain maintenance in coordination with GTA operations.
Agency	• Formulates requests for domain maintenance.
GTA	• Reviews recommendations from GADAC and GEITLF and makes decisions.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, GTA, or Outsource Vendor	1. Submits a request to change a Domain to GTA.
GTA	2. Assigns a tracking number and forwards the request to GADAC.
GADAC	3. Reviews the request and prepares a formal recommendation to be submitted to GTA for reconsideration within 60 days.
GTA	4. Provides a response on the status of the request to the GADAC and the originator. 5. Instructs the Outsource Vendor and/or GTA Operations to make the change.
Outsource Vendor and/or GTA Operations	6. Assigns resources; develops a schedule.
GTA	7. Approves the suggested schedule.

Outsource Vendor and GTA operations GTA	8. Performs requested action, if approved, within approved schedule. 9. Checks with request originator to ensure that the change met identified needs. 10. Requests will be retained by the Outsource Vendor for a minimum of 1 year.

7. EXCEPTIONS

No exceptions as of this revision date.

8. REFERENCES

- Review Cycle
- Exemption Request
- Domain Policy
- GADAC Standard

8.1 Information to be Included

As much detail as possible should be included in each request. The following items must be included at a minimum.

- Description of add/change/delete
- Justification based on business need
- Necessary timeframe for completion or implementation
- Contact information for the request originator
- Scope of change
- Any prerequisites or coordination requirements
- Agency authorizing party signature or indication of approval

Exemption Request

Topical Area: Exemption Request	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to request exemptions from the active directory standards and procedures specified for the State of Georgia.

2. SCOPE

All proposed changes to active directory that do not follow standards and procedures for the State of Georgia.

3. RATIONALE

There must be a process that allows an agency to request an exemption (variance) from established standards and procedures, given a reasonable business case. This procedure outlines the steps that must be taken to apply for such an exemption.

4. DEFINITIONS

4.1 Georgia Active Directory Advisory Committee (GADAC) – The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Georgia Enterprise Information Technology Leadership Forum (GEITLF) - An advisory committee comprised of high-level IT staff from select agencies that advise on enterprise IT issues.

5. RESPONSIBILITIES

GTA	• Receives, routes for review, and makes decisions on exemption requests.
GADAC	• Reviews and makes recommendations on exemption requests.
GEITLF	• Optionally reviews and makes recommendations on exemption requests.

Exemption Request

Topical Area: Exemption Request	Standard Number:
Effective Date:	Revision Date: 10/1/2002

6. PROCEDURE

RESPONSIBILITY	STEP
Agency	1. Completes and delivers the request for exemption to GTA. The request should include a description, business case and time frame for granting the exemption, contact information, authorized signature, scope, and cost (if known).
GTA	2. Issues tracking number, routes the request to GADAC and notifies agency that it is being reviewed by GADAC.
GADAC	3. Reviews the request and sends its recommendations, including reasons for acceptance or rejection, to GTA within 60 days.
GTA	4. Decides whether to grant or reject exemption and sends decision to agency.

7. EXCEPTIONS

A Request for Exemption may also be sent to GEITLF for comment.

8. REFERENCES

- GADAC Standard
- Review Cycle

Naming Standard

Topical Area: Naming Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the naming conventions that must be used for various elements in active directory for the State of Georgia.

2. SCOPE

All specified objects in the active directory structure for the State of Georgia.

3. DEFINITIONS

3.1 Group Policy Objects

Group Policy Objects may be created and deployed in a Windows 2000 server environment much the same way as SMS. They are application objects that can be linked to users and used to remotely deploy applications.

3.2 SMTP (Simple Mail Transfer Protocol)

The Internet electronic mail protocol

4. STANDARD

4.1 Workstation Naming Standard

- The Outsource Vendor assign workstation names of length of 15 hex characters.
- Workstation name must be specified on asset tag unless a security risk dictates otherwise.
- Web access of information for application help and on asset tag.
- Consideration is given to using asset management software.

4.2 Domain Naming Standard

Organization acronym, followed by State Root Domain placeholder. For example DHR.AD.GA.GOV.

Maximum values apply and should not exceed 15 characters. No special characters should be used.

4.3 Server Naming Standard

Servers shall be named with a string containing a maximum of 15 characters and constructed as follows (working from the left):

- An agency code in 3 or 4 characters that is managed by the GTA
- A two character function code that is managed by the GADAC. See section 5.1 for codes.
- A 3 digit sequence number assigned by the outsource Vendor
- A hyphen
- A 5 or 6 character optional description code as managed by the Agency. The Agency can indicate here, e.g., whether the server is production or development. The string shall contain neither blanks nor special characters. For example: GTAFS007-DOCS.

.

4.4 Site Naming Standard

Sites shall be named with a string containing a maximum of 255 characters and constructed as follows (working from the left):

- The city
- A hyphen
- The site description

The string shall contain neither blanks nor special characters.
For example ATLANTA-TwinTowers

4.5 User Login Ids

4.5.1 Non-Administrative Accounts

- The User login name/User Principal Name (UPN) is formatted as first initial, full last name (*see note) @ organizational acronym, followed by State Root Domain name. For example jdoe@gta.ad.ga.gov. Length and duplicate handling follow the NetBIOS login name definition.
- NetBIOS login name or Pre-Windows 2000 login name would reflect first initial, full last name and follow the conventions below.
- Total characters not to exceed 15; truncate within last name to avoid using more than 15 characters.
- Duplicates should be handled by the following, in sequence
    - Add middle initial
    - Add next letter of first name
    - Append a sequence number if still not resolved

- User accounts require the following attributes be filled in using the following formats
  - First Name
  - Last Name
  - Initials
  - Display name – formatted as Last name, First name followed by agency acronym for duplicate display names. If there are duplicates even with agency acronym add division or other identifier to eliminate duplicates. Examples would be Smith, John – Smith, John (DHR) – Smith, John (DHR-DFCS)
  - Address
  - City
  - State
  - Zip Code
  - Company to contain the GTA maintained Agency codes
  - Department to contain agency division or work group as defined by each agency
  - Office Phone number
  - E-mail address
  - Manager must be populated if present on E-form
  - Other phone/pager/fax numbers must be populated if present on the E-form

4.5.2 Administrative accounts

- The User login name/User Principal Name (UPN) is formatted as "!", first initial, full last name (*see note) @ organizational acronym, followed by State Root Domain name. For example !jdoe@gta.ad.ga.gov. The "!" prefix indicates an administrative account.
- Total characters not to exceed 15; truncate within last name to avoid using more than 15 characters.
- Duplicates should be handled by the following, in sequence
  - Add middle initial
  - Add next letter of first name
  - Append a sequence number if still not resolved
- User accounts require the following attributes be filled in using the following formats
  - First Name
  - Last Name

- Initials – may be blank if person does not have middle initial
- Display name – formatted as Last name, First name followed by agency acronym for duplicate display names. If there are duplicates even with agency acronym add division or other identifier to eliminate duplicates. Examples would be Smith, John – Smith, John (DHR) – Smith, John (DHR-DFCS)
- Address
- City
- State
- Zip Code
- Company to contain the GTA maintained Agency codes
- Department to contain agency division or work group as defined by each agency
- Office Phone number
- E-mail address
- Manager must be populated if present on E-form
- Other phone/pager/fax numbers must be populated if present on the E-form
- User Login Name/User Principal Name

4.5.3 Service Accounts

Service Accounts should begin with "**svc-**" agency code prefix (e.g., dot) followed by a hyphen and a name that describes the service it supports (e.g., Svc-dot-Meterman). The Description should contain the ID of the owner/requestor of the service account.

The account options **User cannot change password** and **Password never expires** should be selected.

Service accounts should be a member of Domain Guest Security Group, unless there is a process justification for membership in Domain Admins. No service account should be a member of Domain Users or any other User Global Group, unless there is a specific process justification.

4.6 E-mail Addresses

4.6.1 User E-mail Address

First initial, full last name (*see note) @ agency code, followed SMTP domain name, which should reflect "First Initial and full lastname@Organization agency code.GA.GOV, for example jdoe@gta.ga.gov

*Total characters not to exceed 15; truncate within last name to avoid using more than 15 characters. For handling duplicates see direction in 4.5.1.

4.6.2 Generic E-mail Addresses

Agency code, hyphen, Department acronym, optional hyphen, optional custom field. For example gta-hr-resumes@gta.ga.gov. Mail enabled accounts may be created and then disabled to keep users from logging on the domain with the account.

4.7 Application Naming Standard

Vendor name acronym, hyphen, product name acronym, hyphen, version, optional hyphen, optional custom field. For example MS-PROJECT-2000-SR1A

Application team to develop list of Vendor acronyms for use in application group object naming conventions.

4.8 Group Policy Object Naming Standard

Agency code, hyphen, business function or location, hyphen, and agency defined optional field.

4.9 Printer Naming Standard

- Agency code (4 characters), “P”, Printer ID (5 digits). For example, GDOTP12345
- The location field is required and should contain a standardized code. Codes must be standardized by the Outsource Vendor, i.e., Building Acronym/Code, hyphen, Floor, hyphen, Division, hyphen, Asset/Inventory Number, followed by fields for Location (room/cube) and Comment (description).
- A comment field is required and shall include information as determined by the individual agency.

*__Note:__ Model attribute must be populated

5. REFERENCES

5.1 Server Function Codes

Topical Area: Naming Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

In cases where the server is multi-functional, the highest priority function takes the name, e.g., a combined domain controller and WINS server will be coded as DC.

Server Function	Code
Anti-virus Server	AV
Application Server	AP
Database Server	DB
Development Server	DV
DHCP Server	IP
DNS Name Server	NS
Domain Controller Server	DC
File Server	FS
Gateway Server	GW
Mail/Messaging Server	MS
Print Server	PS
Proxy Server	PX
Remote Access Server	RA
Remote Installation Server	RI
System Management Server	SM
Terminal Server	TS
Utility ("catchall") Server	UT
Web Server	WW
WINS Server	WN

Organizational Unit Standard

Topical Area: Organizational Unit Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To communicate standards for implementing an active directory Organizational Unit (OU) structure.

2. SCOPE

Agencies of the State of Georgia that have implemented active directory.

3. DEFINITIONS

3.1 AD Structure Standard - A standards document that includes the top-level OU design for the State of Georgia.

3.2 Georgia Active Directory Advisory Committee (GADAC) - The body that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for Active Directory policies and operations within the Georgia enterprise computing environment.

3.3 Georgia Enterprise Information Technology Leadership Forum (GEITLF) - An advisory committee made up of high-level IT staff from select agencies that advise on enterprise IT issues.

3.4 Organizational Units (OUs) - Containers that are used to organize objects, such as users, computers, and groups, within an active directory domain. OUs are distinct logical administrative units that are used to delegate administration within a domain.

4. Standards

4.1 Reasons for Creating OUs

When designing an OU hierarchy, the focus should be on reflecting the organization's business model. The benefit of the OU hierarchy may be enhanced administrative control, high granularity of policy application, and logical organization of the objects contained in active directory.

4.1.1 Enhanced Administrative Control

Distribution of network administration can be achieved by delegating administration to an OU:

- An OU can also be used to keep objects with identical security requirements together, thereby simplifying object administration.

- An OU controls the visibility of objects, such as users, computers, and groups. It also makes resource administration more efficient. For example, one can assign permissions once for an OU with many shares rather than multiple times for each share.

4.1.2 Policy Application

An OU can control a policy application as it applies to a distinct group of users or computers. Policies can apply to a Site, Domain or individual Organizational Unit.

4.1.3 Object Structuring

Although there is no practical limitation to the number of objects that may exist in an OU, it is recommended that the number be limited for simplicity of end-user browsing.

4.2 Additional Design Considerations for OUs

For consistency, it is recommended that first-level OUs be standardized throughout the organization, although OU hierarchies are unique to a domain.

- LDAP searches are degraded by a large number of OU levels. The more shallow the OU hierarchy, the better the search performance. Therefore, no more than 10 levels in a hierarchy are recommended.

- The number of OUs, or depth of the OU hierarchy, will have a negligible impact on replication. Delegation of administration at the OU level, as opposed to the object level, will be easier to track and manage, thereby reducing administrative costs.

4.3 OU Models

The OU hierarchy should be beneficial and meaningful. *Do not create OU structure for the sake of structure*. OU Design proposals must reflect one of the listed OU models or a hybrid combination of several models.

4.3.1 Geographic Hierarchy

A geographic model structures OUs along stable geographic boundaries. For example, first-level OUs may be based on counties (e.g., Fulton,

Dekalb, or Cobb); second-level OUs on cities; and third- level OUs on specific locations.

Advantages:

- First-level OUs may not change as often as with other models because geographic boundaries generally remain stable.
- OU administrators can easily identify the physical location of resources.

Disadvantage:

- The design may not mirror the organization's actual business practices.

4.3.2 Organizational Hierarchy

An organizational model structures OUs along business units. For example, first-level OUs may represent the organization, while second-level OUs may represent sub-businesses.

Advantages:

- It is user-friendly because it builds upon knowledge that users already have.
- It is easy to browse and query to obtain required information because resources are in clearly defined locations.
- Unique business policies can easily be applied to the appropriate business units.

Disadvantage:

- It may require restructuring if a division or business unit is renamed or reorganized.

4.3.3 Object-based Hierarchy

An object-based model structures OUs along object classes (e.g., users, computers, or groups).

Advantages:

- It makes resource administration easier because OUs are designed by object type.
- It is easier to create common access control lists (ACLs) for object classes.
- Resource administration can be customized according to the various levels of the OU administrator because OUs are designed by object type.

For example, it would be easy to grant appropriate permissions to "Account Operators" on OUs that contained only user accounts and to "Print Operators" on OUs that contained only printer objects.

Disadvantage:

- Potentially, there are a large number of object OUs.

4.3.4 Project-Based Hierarchy

A project-based model structures OUs along corporate projects.

Advantages:

- This model can provide an easy method for tracking costs and expenses, when separating objects by project is mandatory.
- This model controls access by creating a separate hierarchy for each project. It could be a good choice if project security is an issue.

Disadvantages:

- Projects have a definite life span that restricts the longevity of an OU.
- Because projects change frequently, maintenance may be high.

4.3.5 Administration Hierarchy

An OU hierarchy can be developed which solely models the administrative model of the organization. For example, a central IT organization can be represented as a first level OU, IT organizations can be represented as the second level, and branch or departmental IT organizations represented at a third level.

Advantages:

- This model makes the system administrator's job simpler because resources are organized from an IT perspective.
- This model makes it easy to identify OU administrators in a domain.

Disadvantages:

- It is division-centric and may be difficult for users because everything appears under one division.
- It might not reflect the way that the organization conducts business.

5. OU Design Approval

OU design proposals must be submitted to the GTA for approval and to the GADAC and GEITLF for review.

Topical Area: Organizational Unit Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

6. REFERENCES

- Exemption Request
- GADAC Standard
- OU Policy
- Review Cycle

Password Reset Standard

Topical Area: Password Reset Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to reset passwords for Authorized Users authenticating to the active directory structure.

2. SCOPE

All passwords contained within the statewide active directory for the State of Georgia.

3. RATIONALE

A controlled and secure method for resetting passwords contained in the active directory is required. This method must take cost into account and must be implemented by agencies and the Outsource Vendor.

4. DEFINITIONS

4.1 Outsource Vendor – The organization that supports the majority of active directory work. Originally chartered in the CCOP Contract (2003).

5. RESPONSIBILITIES

Outsource Vendor	Performs steps to create and safeguard log files for Outsource Vendor-supported servers.
Agency	Performs steps to create and safeguard log files for outsourced agency-supported servers.

6. PROCEDURE

RESPONSIBILITY	STEP
User	1. Makes initial request by calling Outsource Vendor helpdesk.
Outsource Vendor Helpdesk	2. Opens a trouble ticket.
Outsource Vendor Helpdesk	3. Validates user request via challenge question. (Agencies may request 1 to 4 challenge questions to be used for their personnel.)

Password Reset Standard

Topical Area: Password Reset Standard	Standard Number:
Effective Date:	Revision Date: 10/1/2002

Outsource Vendor Helpdesk	4. Resets password to random selection and closes trouble ticket.
User	5. Logs in and selects a new password.

7. EXCEPTIONS

No exceptions as of this revision.

8. REFERENCES

- Password reset (available 24 hours a day, 7 days a week)
- Review Cycle
- Security Policies

9. INFORMATION

Tracking - Information should be available online to generate report.

1. Track requests by:
   - User
   - Agency
   - Date
   - Time
2. Track time of password change (open ticket to closed ticket).
3. Use a feedback mechanism to survey user satisfaction.
4. The Outsource Vendor will not approve password change for the same person more than twice within 24 hours without auditable supervisor approval or authorized agency contact approval.

Review Cycle

Topical Area: Review Cycle	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To ensure that the state's active directory policies, standards, and procedures remain effective.

2. SCOPE

All policies, standards, and procedures pertaining to active directory.

3. DEFINITIONS

3.1 GADAC – Georgia Active Directory Advisory Committee - Advisory group that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4. STANDARD

4.1 Annual Review

All Active directory policies, standards, and procedures should be reviewed annually by the GADAC to ensure that they continue to meet industry best practice and design guidelines.

4.2 Backups

Any agency or Outsource Vendor proposed changes should be recommended to and reviewed by the GADAC and/or GEITLF committees and voted on for submission to the GTA.

4.3 Time Line

Proposed changes to active directory policies, standards, or procedures should be approved or rejected within 60 days of its submission date.

4.4 GADAC – Georgia Active Directory Advisory Committee - Advisory group that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.5 GEITLF – Georgia Enterprise IT Leadership Forum – an advisory committee made up of high level IT staff from selected agencies to advise on enterprise IT issues.

5. RESPONSIBILITIES

GADAC	• Performs a technical review of all policies, standards, and procedures and make recommendations to GTA through GEITLF • Routes changes through GEITLF
GEITLF	• Reviews recommendations made by GADAC and pass to GTA
GTA	• Accepts or rejects changes • Tracks change requests • Moves changed policies, standards and procedures through the approval process.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, Outsource Vendor, or GTA	1. Submits proposed changes to policies, standards, and procedures to GTA
GTA	2. Assigns a tracking number and routes all proposed changes to policies, standards and procedures to GADAC
GADAC	3. Assigns a liaison to monitor progress of proposed changes. 4. Performs a technical review of all policies, standards, and procedures and make recommendations to GTA through GEITLF within 30 days. 5. Sends out proposed changes to the list server 6. Routes changes through GEITLF
GEITLF	7. Reviews recommendations made by GADAC and pass to GTA

GTA	8. Accepts or rejects changes. 9. Moves changed policies, standards and procedures through the approval process.

5. REFERENCES

- GADAC Standard

Schema Change Procedure

Topical Area: Schema Change	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the steps that must be performed to request a schema change in active directory for the State of Georgia.

2. SCOPE

The active directory for the State of Georgia.

3. RATIONALE

Given the fact that there is one schema for the state, it is vital that an effective procedure for making schema changes.

4 DEFINITIONS

4.1 GADAC – Georgia Active Directory Advisory Committee - Advisory group that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – Vendor charged with supporting the majority of active directory work. Originally chartered in the CCOP Contract in 2003.

4.3 GEITLF – Georgia Enterprise IT Leadership Forum – an advisory committee made up of high level IT staff from selected agencies to advise on enterprise IT issues.

5. RESPONSIBILITIES

GADAC	• Performs a technical review of all change requests and make recommendations to GTA through GEITLF
GEITLF	• Reviews recommendations made by GADAC and pass to GTA
Outsource Vendor	• Formulates requests for changes
Agency	• Formulates requests for changes

Schema Change Procedure

Topical Area: Schema Change	Standard Number:
Effective Date:	Revision Date: 10/1/2002

GTA	• Forwards proposed changes to GADAC and implements changes
GADAC Chairperson	• Communication on proposed active directory policy, standard, and/or procedure changes should be sent out via the list server to all current GADAC committee members.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency	1. Submits a schema change request to GTA.
GTA	2. Assigns Control Number for Tracking within 2 business days.
	3. Submits to GADAC for review.
GADAC	4. Recommends approval/disapproval to GTA, with reasons.
GTA	5. Reviews and decides on change request.
GTA	6. Notifies sender of approval/disapproval within 2 business days of decision.
GTA	7. Performs testing– and documents change in Schema Change log.
GTA	8. Sets date for change implementation, with a 2- week lead time. The change should be made during non-peak usage times, with at least 1 non-business day following day of change.
GTA	9. Notifies all agencies of upcoming change and date (minimum of 2 weeks notice).
Agency	10. Any agency with an objection to the date should state immediately.
GTA	11. GTA will repeat notification 1 day before change.
GTA	12. Implements change
GTA	Notifies agencies of success or failure of change. If failed, GTA should specify what remediation steps were taken.

Schema Change Procedure

Topical Area: Schema Change	Standard Number:
Effective Date:	Revision Date: 10/1/2002

7. EXCEPTIONS

No exceptions as of this revision date.

8. REFERENCES

- Exemption Request
- Forest Policy
- Review Cycle
- Security Policies

Tracking

A schema change log should be created. A new entry for each requested schema change should be logged with all documents provided per information section. An electronic copy of the log will be retained for 5 years, to be reassessed as necessary.

Security

Topical Area: Security	Standard Number:
Effective Date:	Revision Date: 10/1/2002

- Under Development -

Security was a major concern of the Georgia Digital Academy on Active Directory (GDAAD). While the standard has not been completed, a significant amount of work has already been done.

See the *Next Steps* section of this final report for more information**.**

.

Site Maintenance

Topical Area: Site Maintenance	Standard Number:
Effective Date:	Revision Date: 10/1/2002

1. PURPOSE

To describe the step that must be performed to make a change in an active directory site for the State of Georgia.

2. SCOPE

All sites used by the active directory structure for the State of Georgia.

3. RATIONALE

The Outsource Vendor will perform the majority of site adds, changes, and deletions to implement changes requested by agencies. They will be responsible for replicating changes to the appropriate servers. A procedure is required to ensure that desired changes are requested, implemented, and tracked in a timely and effective manner.

4 DEFINITIONS

4.1 GADAC – Georgia Active Directory Advisory Committee - Advisory group that reviews proposed changes to active directory and makes recommendations to GEITLF and/or GTA for active directory policies and operations within the Georgia enterprise computing environment.

4.2 Outsource Vendor – Vendor charged with supporting the majority of active directory work. Originally chartered in the CCOP Contract in 2003.

4.3 GTA Operations – The Information Resource Management branch of GTA that manages the active directory root domain.

4.4 GADAC Chairperson – Elected chair person of the Georgia Active Directory Advisory Committee.

5. RESPONSIBILITIES

GTA Operations	• Tests and implements schema changes.
GADAC	• Performs a technical review of all change requests and makes recommendations to

	GTA.
Outsource Vendor	• Can request schema extension and is responsible for ensuring that all domain controllers get the new schema.
GTA	• Tracks and makes final decision to implement schema changes.

6. PROCEDURE

RESPONSIBILITY	STEP
Agency, GTA, or Outsource Vendor	1. Submits a request to change a site to GTA.
GTA	2. Assigns a tracking number and forwards the request to GADAC.
GADAC	3. Reviews the request and prepares a formal recommendation to be submitted to GTA for reconsideration within 60 days.
GTA	4. Responds to the GADAC and the originator of the request with status. 5. Instructs the Outsource Vendor and/or GTA Operations to make the change.
GTA Operations	6. Tests schema change.
Outsource Vendor and/or GTA operations	7. Assigns resources, develops a schedule
GTA	8. Approves the suggested schedule.
Outsource Vendor and/or GTA Operations	9. Performs requested action if approved, within approved schedule.
GTA	10. Checks with request originator to ensure that the change met the originators needs.

7. EXCEPTIONS

No exceptions at the time of this revision.

8. REFERENCES

- Exemption Request
- GADAC Standard
- Review Cycle

- Site Policy

8.1 Information to be included in every request

As much detail as possible should be included in each request. The following items must be included at a minimum.

- Description of Add/Change/Delete
- Justification Based on Business Need
- Necessary Time Frame for Completion or Implementation
- Basic demographics (location, number of users)
- Site plan
- Contact information for the request originator
- Scope of change
- Any prerequisites or coordination requirements
- Agency authorizing party signature or indication of approval

8.2 Tracking:

(Information should be available online to generate report.)

1. Requests and log will be viewable on GTA's website current within 4 business days
2. GTA will maintain a permanent change log, available to agencies for viewing via web.

6. GEORGIA ACTIVE DIRECTORY PROFESSIONAL ASSOCIATION (GADPA)

(To Be Done: At this point, this section is more in the form of "notes." It is anticipated that details about the following major items will be provided during the electronic and face-to-face review sessions.)

6.1 WORK PLAN

6.1.1 Host
6.1.2 Activities
6.1.3 Deliverables
6.1.4 Outputs
6.1.5 Inputs
6.1.6 Benefits

In keeping with our recommendation to continue building a professional community of interest for AD we describe in this section our planned actions to form a user group for AD professionals.

Membership: We want to include AD professionals from the GTA, all State agencies, all levels of government, all Industry, all education, and other organizations to ensure effectiveness. It is our intention to smoothly blend the work of the GTA, GADAC, and GDAAD user group as well as all AD professionals.

Initial organizing meeting: 10/29/02 at Southern Polytechnic

Organizing Committee: We want to establish an organizing committee to complete the tasks of organizing the group. As of the writing of this report, we have three GDAAD participants who have volunteered to serve on the committee: Leah Davis, Stephen Diggs, and Dennis Reynolds. On 10/1/02, we will ask for additional volunteers and set a schedule for the organizing committee.

Sponsor for the Organizing Committee: GTA

Logistics and Advisory Support for the Organizing Committee: SPSU

Resources:

- Continuation of the GDAAD listserve and web site
- A Recorder (Doris Konneh).

Additional provisions:

- A desire to be a "professional association" for professionals working with active directory.

- A desire to utilize the experience and plan of the Georgia Document Management Association, e.g., to use the PMI User Group Template.

7. GEORGIA ACTIVE DIRECTORY PILOT PROJECT

The state plans to outsource desktop and most LAN server based support. GTA convened the digital academy on active directory to delineate the desired state that the vendor must implement for the state. Their charge was to write the policies, standards, and procedures that the state desires in the new outsourced environment. In order to test drive these new policies, standards and procedures, a pilot project was commissioned. The entire production staffs of GTA, DOAS, and GDOT will be involved in the pilot. This involves about 5,000 user accounts and 70 locations. The pilot starts with the ongoing move of GTA into the new active directory structure. DOAS will be separated from the GTA infrastructure and workstations will be upgraded as a second part of the pilot. GDOT will convert from its NT4 and Exchange 5.5 environment as the third component of the pilot. The end date for the pilot is June 30, 2003 when the CCOP vendor takes over operations.

7.1 Phases

The pilot will be done in two phases:

Phase 1 - Move the production staffs of the three agencies into the single statewide forest with a domain for each agency that contains all their desktops, users, and servers. This will be done per the policies, standards, and procedures developed in the GDAAD with a few exceptions that will be documented and reviewed by the GADAC. The target date for the end of this phase is January 2003.

Phase 2 - Test the moving of all but the out-of-scope servers from the agency domains into a single accounts domain with organizational units for each agency per the AD Structure standard. The idea is to establish a pseudo-CCOP environment to further test the policies, standards, and procedures. The format of this test is still being developed.

7.2 Benefits

In all probability, the templates set up in the pilot will be close what is done after the CCOP vendor takes control. The lessons learned in the pilot can be worked into the agreement with the CCOP vendor to make a more effective relationship. GADAC will review all changes to policies, standards, and procedures that are recommended from the lessons learned.

Another benefit of the pilot is to set up the root domain in a production manner with the required disaster recovery and other processes in place. We will have 8 months or so experience running the root domain before we start moving massive numbers of accounts into the single forest.

8. CONCLUSIONS

Based upon the work of the GDAAD effort, the following conclusions were reached:

- To achieve integration of the individual agencies' IT assets into a coherent statewide enterprise, communication between the agencies is key.
- Developing a statewide AD structure requires the adoption and adherence to well-structured and appropriate standards.
- A formal and proactive governance process (GADAC) must be in place to ensure the standards are implemented and continuously improved.
- In the CCOP environment, the role of agency IT personnel changes from one of direct operations and implementation to the management of the implementers/operators (CCOP vendor).
- The single-forest model appears most likely successful for a statewide enterprise IT structure.
- Security is and always will be a top-priority consideration in the statewide implementation of AD.
- Convenient access to the statewide enterprise is and always will be a top-priority consideration in the statewide implementation of AD.
- Many of the decisions and actions made by the State AD professionals will involve trade-offs between security and convenient access in the statewide implementation of AD.

9. RECOMMENDATIONS

The GDAAD proposes two sets of recommendations to the GTA regarding both directory services and the conduct of the corresponding sessions of the Georgia Digital Academy:

- Recommendations based on conclusions
- Recommendations based on input from the final evaluation

9.1 Recommendations based on Conclusions

- A single forest model should be implemented in the State of Georgia.

- Continue building a professional community of interest for AD. Include GTA, State agencies, Industry and other organizations to ensure effectiveness. Smoothly blend the work of the GTA, GADAC, and GDAAD user group.

- Continue building and refining a governance structure for administering and operating AD for the statewide enterprise.

- The GTA should formalize and publish a process for IT standardization that includes policies, standards, procedures, guidelines, best practices, etc.

- A formalized change and migration process should be established in support of CCOP to facilitate the movement of Agency IT personnel from operations roles to vendor management roles.

- A formalized, efficient, and effective training and communications module should be developed and implemented for GDA participants. This module should describe the role of all players—the GTA, SPSU facilitators, participants, SMEs, etc.—and should be delivered prior to future GDA sessions. This module's main purpose will be to synchronize all parties to a common point of departure and set appropriate expectations.

- Identify and implement opportunities for cross-GDA activities. For example, the GDAAD developed a pilot security survey that could be implemented jointly with the Georgia Document Management Association (the user group from the GDA on document management).

9.2 Recommendations based on Final Evaluation

- Maintain open communication with the agencies on all issues that affect enterprise technology.

- Continue efforts to foster agency interaction, as it is vital to the success of GTA's initiatives.

- Expand the one-on-one agency consultation session (also known as the Wednesday session) and make it mandatory rather than optional.

- Continue the team approach to task completion - small group assignments with ultimate approach by the larger group. This method seems most productive.

- Ensure that planning remains a key feature of active directory implementation.

- Expand the number of days for structured classroom training.

- Schedule the Academy at another time of the year. Summer is an extremely busy time.

- Include participants with a more diverse mixture of skill sets (e.g., both technical and managerial).

- Expand the number of agencies required to participate in the Academy.

- Implement more pre-planning sessions [for the Academy] involving both management and technical team members.

- Provide more specific information on how CCOP [the Outsource Vendor] will impact the agencies.

- Place more emphasis on technical hands-on issues, such as migration, and less on paperwork (e.g., procedures).

- Ensure that all GTA personnel (from the top down) communicate consistent information.

- Provide opportunities for direct interface between the agencies and the Outsource Vendor.

10. NEXT STEPS

- The GTA should maintain a tracking system that the agencies, GADAC, GEITLF, and the Outsource Vendor can use to view and as appropriate update requests. This should be planned by 11/1/02 and implemented by 1/1/03.

- The GADAC should review and finish the AD Security Standard and deliver the results to the GTA by 11/12/02.

- The GADAC should work on a Service Level Agreement Standard and deliver to the GTA by 11/5/02.

- The GADAC should develop an AD Schema Testing Standard and deliver to the GTA by 2/1/03.

- The GTA should keep SMEs with Microsoft AD expertise on retainer as long as needed.

- The GTA should administer and appropriately publish the Security Compliance Survey by 1/1/03.

- The GADAC should develop Form and Report content as appropriate to the AD Standards by 11/05/02.

- The GADPA should align AD activity and train AD professionals for auditability; e.g., in GTA Security Policies. This training activity should be started by 4/15/03.

- The GADPA, GADAC, and GTA should work in concert to get ALL Georgia State agencies and Authorities involved in the GADPA and GADAC. This activity should be started in October 2002 and remain ongoing.

- The GTA should appoint an SME for AD Security to interact with the GADAC and GADPA by 11/1/02.

  The input from the GDAAD on security is included below, primarily in the form of "notes." This input will be reviewed in light of the newly published security policies, placed in the correct format, and passed through the GADAC for approval.

Availability Security Standards

GDAAD Homework Submission for 8/6/02 Session

- Backup
- Redundancy
- Disaster Recovery

backup	redundancy	disaster recovery
Frequency	What is Included	Off site Location
Retention	Domain Controller	Plan
Location	Monitoring & Notification	Periodic Testing
Access	Monitoring & Notification	Monitoring & Notification
Tape Handling		
Restore - time		
Testing backup		
Monitoring & Notification		

Redundancy

- There will be at least two domain controllers for the root forest directory
- Audit logs will be maintained and will be reviewed for functionality daily

Backups

∃ There will be a full backup of the forest root daily.

∃ AD backup must be enabled (@forest root).

∃ Tape will be retained for 35 days

∃ Tape expires after 45 days

Georgia Digital Academy: Active Directory
Homework from session held on 7/30/2002

Charge: Standards for Network Security (Active Directory)

The AD group came up with the following points to discuss for Network Security:

- **Date Security**
  -Encrypt Sensitive Data
- **Data Storage**
- **Data Communication**
  -AD
- **Directory Services**
  -Domain
    account management
  -Forest
    account management
    background checks on admins
  -OU

After the AD group separated into the Network Security group, the Network Security group concurred that development of network security should be for AD only.

AD Security Brainstorming Concepts		
Topic	**Bullet Points**	**Comments**
Access (general)	• Who	
	• What	
	• When	
	• Where	
	• How	
	• Why	
Documented Authorization	• Length of time	
	• Limits (external/internal)	
Password (policy, standard, procedure)		
Auditing		
Disabling Accesses	• Inactivity	
Encryption AD Database	• How	
	• Update, e.g., 128 to	
	• Where takes place	
	• Where-to-where	
	• To meet Fed Regs	
Admins Selection Regs	• Individual Access	
	• Background check	
Topic	**Bullet Points**	**Comments**
Account Management	• Difference b/t Domain & Forest?	Tim from MS said treat as same
	• Roles	
	-Agency	

	-CCOP	
	-GTA Rep	
	• IPSec	
	• Certificates	
	• Card Access w/PKI	
	• Document justification & records (auditing)	
	• Notification of personnel changes	
	-most importantly disabling accounts	
	-critical data access	
	• In/out scope accounts	
Group Policy	• Min regs	
	• What information is stored about each account	
Schema Security (in GADAC)	• or say “leave alone”	
AD Network Security Standards Layout		
Start with Forest		• Develop standards and work our way down
		• Make assumptions & document them
Physical Security		• Assume covered in other meeting
Setting up Admins (Forest Level)	• Background check	
	-Financial	
	-Polygraph (on demand)	
	-Fingerprint	
	-Drug/alcohol (random)	
	-References	
	-Travel history/passport	
	-Approval by GADAC	
	-Enterprise/Schema Adminis should be state employees	
Admins Documentation	• who	• Circulate to appropriate information officers
	• Role	
	-Authority (what they can do)	

	-Scope	
Topic	**Bullet Points**	**Comments**
Admins Audit	• Anything	• Need auditing tools (MS Operations Manager)
	• Reviewed by the Dept of Audits	
	• Retention period	
	• Review period	
Questions	• What is CCOP responsible for with respect to security?	
	• What is GTA's security policy or proposal?	

C:\CJCC\GADAHomework.doc
07/31/2002

GDAAD Homework from August 6, 2002

Additional Topics for the Network Security Standard

Password Policy

1. Minimum of 8 Characters
    a. Upper & lower case
    b. Numbers
    c. Special Characters

2. 30 Day Expiration

3. Can not repeat the past 24 passwords

4. Initial password must be changed at first logon

5. Must be reversibly encrypted

6. Users/Admins must not share passwords

7. Need to set qualifications for administrators who has permissions change passwords

8. Requests for changing passwords
    a. Validated Change/Reset must be implemented within in "real time"
    b. Need a set security validation process (ex. Mothers maiden name, city of birth, social security number, pet's name, etc.)

9. Disable accounts inactive for 90 days

10. Automatically rename administrator account

11. Deactivate Guest Account

12. General Administrator account can not be used to test for monitoring/logging purposes

13. Lockout accounts after 3 unsuccessful tries within 1 hour and an administrator must reset

14. No “Stupid Notes” recording passwords (ex. Sticky note on monitor with password)

15. Limit number of Concurrent Logins
16. Option: Limit logins to specifically machines for specific users
    a. Special access
    b. Temporary Employees

17. Disable accounts & access within a time limit (ex. Disable an account immediately if a user has been let go from their current position)

Other comments: Technical – Use IPSec across domains

Compliance Policy

1. Triggering Compliance Audits/Reviews (ex. Prior to deploying AD change)
    a. Legislation
        i. Section 12 of ISO 17799
        ii. Research/Poll all agencies for legal requirements
        iii. Open Records Impact – Network Impact?
        iv. Intellectual Property
        v. Privacy
        vi. Cryptographic Controls
        vii. Evidence
    b. Auditors requests/schedule
    c. Rule Changes (ex. FHWA)
    d. CCOP Requests
    e. GADAC Requests
    f. Agency Requests

These can be broken down by External/Internal and Mandated/Request lists.

2. Request GDAAD Poll and GTA Poll for All State agencies
    a. Legal Requirements that effect data/network implementation

b. Definition of the requirements
c. Agency compliance process

3. Questions for GTA
    a. Has compliance information been gathered?
    b. What are GTA's / Georgia's compliance requirements?

GDAAD Physical Security from 7/30/02

I. Physical Access
    Locked racks
    Disable drive access (locks keylocks)
    UPS
    Backup Generator

II. Environmental Control
    Flood, temperature
    Fire
    Theft

III. Accountable Access
    Key cards
    Scans
    Biometric
    Guest access
    Cleaning crew access

11. TERMS AND DEFINITIONS

- Agency Domain - A child domain in the Enterprise Forest that serves an individual agency. Sub domains from this child domain may be created at the request of the agency and upon recommendation by the GADAC.

- Agency Forest(s) - Second and subsequent forests that may be created in the Georgia active directory implementation. Such forests would have to be approved exceptions to the Georgia Forest Policy.

- CCOP - Converged Communications Outsourcing Project.

- Dis-Entanglement - A term used to refer to a clause in the CCOP bid documents that allows the State of Georgia to repurchase any assets transferred to the CCOP vendor.

- Domain Administrator - Those AD user accounts belonging to any Domain Administrators global group, Schema or Enterprise Administrators global group, and anyone possessing the password to a user account used to log in as an operating system service.

- Enterprise Forest - The first forest created in the Georgia active directory implementation.

- Enterprise Forest Root Domain - also known as “EFR”. The root domain of the Enterprise Forest.

- GADAC – Georgia Active Directory Advisory. A group of agency technical representatives organized to review and make recommendations on how to manage the active directory implementation to the Georgia Technology Authority.

- GEITLF - Also known as the "Get-A-Life Committee". Georgia Enterprise Information Technology Leaders Forum. An existing committee of agency employees who coordinate with the Georgia Technology Authority on broad information technology issues.

- The Microsoft Active Directory Glossary can be found at http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/glossary.asp

APPENDICES

- Appendix A – Enterprise Technology Policies, Standards, & Guidelines: A Definition

- Sections 6.2, 6.7, and 8 of the Outsource Vendor (CCOP) Request for Proposals (RFP) were also used as source materials. A copy of the RFP can be found at http://www.gagta.com.

- The GADAC web page can be found at http://ad-sharepoint.gagta.com.

APPENDIX A

Georgia Technology Authority

ENTERPRISE TECHNOLOGY
POLICIES, STANDARDS, & GUIDELINES: A DEFINITION

Website: http://www.gagta.com/

GTA ENTERPRISE TECHNOLOGY
POLICIES, STANDARDS, & GUIDELINES: A DEFINITION

INTRODUCTION

In the context of information technology, the words policy, standard, and guideline are often used interchangeably. The intent of this document is to 1) provide working definitions for each of these terms as used by the Georgia Technology Authority ("GTA"); 2) identify which state entities are affected by these terms; and, 3) how they are affected. A thumbnail definition of each term:

- **Policy** – A general statement of direction and purpose; a guiding principle for the management of technology and technology resources.
- **Standard** – A specific directive, specification, or procedure that must be followed.
- **Guideline** – A Guideline is similar to either a Standard or a Policy, in that it outlines a specific principle, direction, directive, specification, or procedure but is not binding. Rather, a Guideline is a recommended course of action.

Enterprise Policies, Standards, and Guidelines related to security, technical specifications, and technology architecture fit within these three categories.

POLICIES

A Policy is a general statement of direction and purpose and/or a guiding principle for the management of technology and technology resources. A specific example of a technology Policy might be:

> *All deployed agency wireless network access environments must adhere to established Georgia Technology Authority Standards applicable to the use of wireless network access technology.*

O.C.G.A. § 50-25-4(a)(10) invests GTA with the authority to "set technology policy for all agencies[6] except those under the authority, direction, or control of the General Assembly or state wide elected officials other than the Governor."

[6] Agency is defined as "every state department, agency, board, bureau, commission, and authority which shall not include any agency within the judicial branch of state government or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11." O.C.G.A. § 50-25-1(b) (1) (Supp. 2001). [Part 4 is now Part 5.] Therefore, the Board of Regents of the University System of Georgia and the Georgia Superior Court Clerks' Cooperative Authority are expressly exempted by statute from GTA's authority as it relates to executive branch agencies, and general references to executive branch agencies within this document do not include them.

Therefore, when GTA issues a technology Policy, it is binding upon all agencies in the executive branch which are not led by constitutional officers.[7] Agencies under the judicial branch; agencies headed by a constitutional officer; agencies under the direct control of the General Assembly; or institutions under the Georgia Board of Regents, can opt to adopt, modify, or ignore the Policy. Further, GTA technology Policies must be approved by the GTA board.

STANDARDS

A Standard is a specific directive, specification, or procedure which must be followed. An example of a technology Standard might be:

> *Strongest available Wired Equivalent Privacy (WEP) encryption shall be employed with maximum key length and shall be upgraded as newer technology is available.*

GTA has the statutory authority to establish architecture for state technology infrastructure; to establish technology security Standards and services to be used by all agencies; and, to establish and enforce Standard specifications which shall apply to all technology.[8] The Attorney General has opined that such Standards apply to all executive branch agencies including those controlled by constitutional officers.[9]

Therefore, when GTA establishes a Standard, it is binding upon all executive branch agencies *including those executive branch agencies headed by constitutional officers*.[10] Agencies under the judicial or legislative branches or institutions under the Georgia Board of Regents can opt to adopt, modify, or ignore the Standard.

ESTABLISHMENT OF STANDARDS

In establishing Standards, GTA will issue draft or proposed Standards for comment by agencies prior to adoption. The purpose of this comment period is to consider, accommodate, and/or include the comments and alternatives presented by state

---

[7] The scope of certain Policies may only apply to agencies that are within a "common community of interest." An example may be certain Policies dealing with HIPAA related data may only apply to agencies that handle certain patient or medical data. The same may be true for certain Standards or Guidelines.

[8] See O.C.G.A. §§ 50-25-4(a) (15), (21), and (29).

[9] In an official opinion analyzing the GTA's authority, the Attorney General opined as follows:

> Viewing the statute as a whole and keeping in mind the legislative intent to consolidate the procurement and management of technology in one agency, it is clear that the ability [of executive branch agencies under the control of constitutional officers] to set technology policy is further constrained by the GTA's authority to establish architecture for state technology infrastructure, establish technology security standards and services, establish and enforce standard specifications applicable to all technology and technology resource related supplies, and establish standards for procurement. O.C.G.A. §§ 50-25-4(a) (15), (22), (29), and (30) (Supp. 2001). (Opinion footnotes omitted). Op. Att'y Gen. 2001-08.

[10] See note 2.

agencies (inclusive of those of under the control of constitutional officers) as well as the legislative and judicial branches of state government. Due to the binding nature of GTA's established Standards on all executive branch agencies, GTA will establish and maintain a procedure to facilitate the comment period and process as an integral part of the Standards establishment process.

GUIDELINES

A Guideline is similar to either a Standard or a Policy, in that it outlines a specific principle, direction, directive, specification, or procedure, but it is advisory in nature. The intent of a Guideline is to promote a "best practice", while recognizing that there may be several ways of accomplishing the same task, or that further analysis is necessary before adoption of a binding uniform approach. It is possible for Guidelines to evolve into Policies or Standards.

An example of a technology Guideline might be:

> *Users should not use easily guessed passwords like wife's name or favorite sports team.*

When GTA issues a Guideline, all agencies are encouraged to follow the Guideline, but ultimately it is the agency's decision whether to use or ignore the Guideline.

CONCLUSION

The application of these working definitions is intended to provide agencies a common framework and perspective on the development of Policies, Standards, and Guidelines. GTA will provide a web-based site for the dissemination of Policies, Standards and Guidelines. Policies will be issued and approved by the GTA Board. The discussion and establishment of Enterprise Standards will be coordinated through the Georgia Enterprise Information Technology Leader's Forum. Guidelines will be issued from time-to-time by GTA, either directly or in conjunction with the Georgia Enterprise Information Technology Leaders Forum.

Cross Functional Services Requirements

The Cross Functional Services Requirements include those Services that are required in support of most or all of the specific Service areas outlined within this SOW. Requirements specific to each Service area are detailed in the SOW sections following the Cross Functional Services Requirements section.

Current Environment

The following describes the current environment of the areas of the cross functional services.

Help Desk Operations:

The State has multiple Help Desk operations typically supporting individual functional areas for individual agencies. The Help Desks are managed to independent objectives using inconsistent policies and procedures. Help Desk call volumes and other statistics are not available.

The State's personnel currently have no single point of contact Help Desk for services provided by GTA, by their agency's internal staff, and/or by vendors. Larger agencies often provide help desk services for their personnel, generally for specific custom applications and desktop support. These help desks or individuals within the agencies often interface with the GTA IT External Help Desk when problems involve the statewide computer system, wide area networks, or other GTA provided services. Support for custom applications including Phoenix, the State's financial and HRMS systems, is generally handled separately by the GTA application development staff and/or help desks set up by the agencies using the custom application. At least one agency has an outsourced first level help desk obtained through an existing GTA contract. This help desk refers unresolved calls to the agency's technical staff or to GTA. Vendors who provide products and services for the State generally provide help desk support for technical staff rather than to all State personnel.

The GTA IT External Help Desk offers 24 X 7 help desk support for the agency's data center services including statewide computer systems, wide area data networking, and PC maintenance contract customers. Calls for these services average approximately 1200 per month, not including status and follow-up calls. The GTA External IT Help Desk dispatches vendors statewide as well as GTA's Installation, Maintenance and Support (IM&S) group, which provides field service statewide for network problems including individual workstation connectivity issues.

GTA uses Peregrine Systems ServiceCenter Call and Problem Management software for all IT and voice troubles. Problem tickets that are not immediately resolved by the help desk are electronically routed to the appropriate group. Severity levels are assigned, followed by notification to the appropriate group. Timeliness of response is tied to notifications. First level help desk call resolution for desktop support is approximately 70% primarily due to the use of a remote desktop management tool. The Board of Regents uses Remedy software for its Help Desk operation.

All voice system troubles are handled by GTA. GTA's Help Desk services for voice are distributed regionally throughout the State of Georgia using a multiple help desk arrangement. The GTA Customer Service Center in Atlanta takes all voice tickets for the Milledgeville and Columbus Regions (approximately 500 to 600 tickets per month). The Atlanta Voice Repair Group, at GTA's IM&S Atlanta facility, takes all voice trouble tickets for the Atlanta Metro Area and surrounding counties (average monthly ticket count is 2300 to 2500). There are five additional voice help desks located in Athens, Rome, Albany, Augusta and Savannah. These regional help desks take an average combined total of approximately 1500 tickets per month. These Help Desks are responsible for taking all customer information, routing problem ticket appropriately to internal groups or to the vendor for resolution, closing tickets and following up with the customer to verify completed repair. All voice Help Desks statewide operate during normal business hours. After hours and weekend voice problem tickets are taken by the GTA External IT Help Desk, which is staffed, 24 X 7.

Change Management Practices:

Change Management practices vary throughout the State. Most processes are manual in nature. GTA manages changes to the IP network using the Change Management module of Peregrine Service Center. Components include a complete description of the change, planned implementation date, personnel assigned, priority, risk assessment and management approval. Task completion notes are updated in the change request with time and date stamps and operator identification as the information is recorded.

Large changes to systems are carefully planned and scheduled. Customer notification of efforts and potential impacts are extremely important, yet are cumbersome to accomplish. As stated earlier, most processes associated with large-scale changes are manual.

Monitoring:

The State's services are monitored by both State staff and our vendors. The State's private network is monitored by GTA's e-NOC. Traffic studies for the network and voice systems are run on a developed schedule for capacity management.

Emergency Responsiveness:

The responsibilities of the State can vary widely during situations of emergency or when incidents occur that impede the State's ability to provide services to its citizens. If a state of emergency or a situation requiring a quick response occurs, state employees take action both proactively and reactively to restore, move, reconfigure or install Services as needed to support the State's mission during these times.

Order Fulfillment:

Order Fulfillment for Services in this RFP is accomplished by multiple methods, depending on the Service required. Customers contact GTA through the Customer Service Center, GTA Region Office or through their GTA Account Manager for Voice, Mobile Short Messaging, Video (GSAMS) and Data Communications. Services such as Distributed Computing, Two Way Radio, Video, and TV Broadcast are obtained through direct contact with the service provider holding the contract for those Services or through various State Help Desks.

For services provided by GTA, a complete description of the change is captured, approved through agency management and submitted to GTA. Approved requests are entered as projects in a PeopleSoft application called PRISM. Work orders and tasks are generated and routed to the appropriate internal units or external vendors for processing. Completion of all work orders associated with a PRISM project is communicated to GTA Customer Service Operations staff through e-mail notification. New circuits installed as part of the managed router service are identified to the Intermapper software for tracking future performance.

Orders submitted to GTA for Installs and MACs are received via fax, e-mail, hand delivery and U.S. Mail and are not generally accepted via phone. All orders must have the approval of the Agency Telecom Coordinator. GTA customer service representatives review the request, work with the customer to gather any additional information required and clarify any points of possible confusion. If it is determined that the request fits the category of a "managed project', it is handed off to the local GTA project coordinator for any necessary site visits and complex design/engineering. On managed projects a formal proposal is sent to the customer for approval prior to the initiation of any formal order fulfillment functions taking place. Intervals for service delivery are negotiated on "managed projects." Standard intervals for delivery are established and adhered to for routine requests.

Following GTA's approval, Services are obtained directly from vendors using contracts or other approved purchasing processes using varying methods to include submittal of purchase orders to the provider.

Wiring & Cable Plant:

Wiring and Physical Plant Maintenance and Installation is a significant part of Installs and MACs, as well as planning and configuring State facilities. The GTA Managed Cabling Program provides expert advice, consulting, design, engineering, and construction project management services for the design and implementation of state-of-the-art telecommunications distribution systems, capable of supporting all currently known telecommunications technologies.

The GTA Managed Cable Services Program ensures customer's telecommunications utility will be installed to support the needs for the typical life of their facility and be flexible enough to accept changes in the future. To do this GTA utilizes its own Building Industry Consulting Services International (BICSI) (www.bicsi.org) Registered Communications Distribution Designers (RCDDs). GTA's staff of RCDDs works directly with architects, planners and building professionals to develop stringent specifications that meet facility occupancy requirements from inception to completion and certification. By partnering with customers, the GTA Managed Cable Service ensures that telecommunications utility needs (voice, data, and video) are met. The RCDD staff serves as the customer advocate insuring installed technology is adequate and properly handled.

The GTA Managed Cable Service Program applies all of the industry standards, such as IEEE, ANSI, TIA/EIA Telecommunications, and GTA's adopted guidelines to meet customer project requirements. RCDD staff is required to meet regular training certification to stay knowledgeable of new trends and complete BICSI approved training

related to industry standards. In depth knowledge of these standards documents allow GTA's RCDD staff to provide Outside Plant (OSP) and Inside Plant (ISP) standardized specifications for customer facilities. An end user review of the scope and specifications prior to construction is provided using these standards to assure correctness and completeness.

The customer base for GTA Managed Cable Services ranges from large university campus environments to local state, city and county entities. When customers choose to allow GTA to engineer and implement their cabling projects, we operate using two specific statewide contracts with vendors to deliver state approved installations. These are the Complex cabling contract, which covers the Outside Plant installations utilizing three pre-approved vendors who competitively bid on each project for materials and labor.

The other contract is the simple contract, which covers inside plant installations and utilizes one vendor who competitively won the statewide bid to provide materials and labor. When using these two contracts for the installation of cabling systems, customers are assured of getting certified trained installation personnel and the latest materials, all of which is managed, reviewed and inspected by the Managed Cable Services staff.

GTA and Georgia State Finance and Investment Commission provide assistance to all state agencies on new buildings or renovations of existing buildings. Provisions have been made to include infrastructure and cabling reviews for agencies with architects, planners, engineers and general contractors at a minimum. Beyond this service (upon customer request), the GTA Managed Cable Services staff has managed the entire cabling project from end to end including the installation and acceptance.

Some GTA customers have elected to use statewide cabling contracts under delegated authority, which allows them to directly use the GTA agency cabling contracts in performing all of the simple and complex contract tasks associated with the project management of wire and cable installations. Under a delegated authority arrangement the agency must adhere to all of the contractual rules outlined in the contracts either on a one time or multiple job basis. This arrangement has had limited success as most agencies do not have trained cabling and engineering staff to manage the projects.

Historically state and other government agencies have not engaged in appropriate planning, engineering and project management at the start of a project thus minimizing opportunities for cost savings.

Equipment & Delivery of Services:

Equipment Staging, Delivery and Testing vary across the state. GTA and other providers work with the customers to minimize disruption. Most instances require staging and testing at the vendor site with turn key delivery at installation.

Once requested Equipment and/or Services have been received and provided to the customer and the different sales order and work assignment "segments" are closed by the Customer Service Representative and the overall "project/work order" is marked for billing.

Billing/Invoicing:

Services provided now by GTA are invoiced to customers monthly. Invoices include recurring and non-recurring charges by Services type. Billing account hierarchy is provided to three levels. Invoices for Services not provided by GTA are generated and sent to customers directly from the Service providers. One of the areas of greatest discontent by GTA customers is accuracy and clarity of billing.

Training:

User Training is provided by State and vendor staff for the Services in this RFP. Varying methods are used to accomplish training delivery.

Contact Center Support:

GTA provides various equipment and services supporting Contact Center operations. A Contact Center is a convergence of technology subsystems used to manage high call volumes. These subsystems include, but are not limited to, IVR, ACD, CTI, wallboards, and predictive dialers. The equipment and services used in each call center varies. The call centers handle inbound call regarding service requests, state park reservations, financial aid support, etc.

GTA provides a stand-alone IVR system integrated with the State's mainframe. This is a 10 group IVR serving multiple agencies including Revenue, Child Support Recovery, State Examining Boards, etc. Contact center sub systems may also include the use of Interactive Voice Response systems.

There are nine (9) PBXs with integrated ACD functionality. Some are providing contact center service to larger constituents, e.g., the University of Georgia with multiple splits/queue groups. Others are only providing service to the contact center's agents, e.g. GTA Customer Service Center. There are ten (10) Centrex based CCMISs. These are in BellSouth's central offices.

Other functionality used in some State contact centers are queuing announcements, multiple-source music on hold, wallboards to display information, such as number of call in queue, average hold time, etc. for agents. Additionally, the State has several licenses and Agent Silent Monitoring/Service Observation systems in contact centers, which allow supervisors to monitor call center agents from remote locations.

Software:

Software used to support Services varies widely as do the methods used to manage it. LAN and desktop software has been historically chosen and managed by each entity. Software for the State's router network, Mobile Short Messaging and Voice systems is either managed by GTA staff or by GTA's provider of services. Other software used for the Services in this RFP are managed and deployed similarly.

Asset Management:

As defined by industry standards, asset management does not presently exist within the State of Georgia. High-level physical asset tracking is practiced and is based on State Auditing requirements. The tracking requirements are centered primarily on item cost with special provisions for certain controlled assets such as firearms. Levels of compliance with these requirements vary from agency to agency.

The State currently uses PeopleSoft Asset Management module as the repository for asset data. Reports generated from this repository are used as base data for State inventory audits.

Efforts at implementing asset management vary by agency. Some larger agencies have invested in auto discovery tools such as Tally NetCensus, SMS and HP Openview. Smaller agencies typically use manual processes based around Excel spreadsheets. The asset data provided with this RFP includes sample data compiled from these various sources.

Refresh Cycles:

Equipment refresh activities are managed on an entity-by-entity basis. Each entity's executive management determines their equipment requirements, follows the documented approval processes, obtains the necessary funding and manages their refresh process. Surplus equipment resulting from refresh activities are transferred to a State authorized disposal center for either purchase by other State entities or sale to the general public.

Security:

The State currently employs a wide spectrum of measures and technologies to protect its information assets, critical infrastructure, and resources. Historically the responsibility for security lay with the individual agencies applying different approaches and tools to this task. For instance, GTA operates multiple redundant state-full inspection firewalls at public network ingress points and an Intrusion Detection system on the IP backbone, while other agencies operate firewalls, virus detection/quarantine systems and perform auditing functions they require on their specific network segments. The creation of GTA provides the means to evolve this disjointed view into an enterprise approach to information security.

Currently, the State enforces security policy compliance, conducts periodic audits, and performs investigations involving misuse of state owned computer systems as specified by the Georgia Computer Systems Protection Act (O.C.G. A. Sec.16-9-90).

Reporting:

Currently GTA receives statistical and analytical reports for Services through a few of its major systems. Peregrine ServiceCenter produces standard and customized reports on Call and Problem Management, Asset Inventory Management and Change Management, along with Customer Contact and Site Location report information.

PRISM produces reports on Order Management, Projects and Group Work Assignments, Items for Resale Inventory, and Billing. In addition, the system has the capability to utilize "system queries" to extract and sort requested criteria for information. These queries are not classified as "standard or custom reports", but serve as an important tool to produce specialized system data. These queries are easily written by the system's super users to fit the desired application.

The State eNOC has systems that produce reports assessing network outages and usage. The Intermapper tool gives real time data and reporting of network outages on the IP network, constantly scanning over 1200 router site locations for problems.

Intermapper also produces real time reporting on Internet usage and availability. In addition, the State has access to our current carriers' tools that monitor T-1 circuits across the State and give real time information on performance, outages and usage. The eNOC obtains network availability and bandwidth usage from a system called Concord Net Health, a proactive monitoring tool that assesses the overall health and welfare of the network from a proactive perspective. Because many entities in the State provide services contained in this RFP, the type and degree of reports obtained and used are unknown.

Desired State

The GTA wishes to improve services through more consistent delivery of services to all users, effective management and integrated delivery of services.

The GTA expects that the Offeror will provide more effective and efficient means of providing Help Desk, Change Management, Project Management, Contact Center Support, etc. due to the Offeror's experience and expertise offering similar services.

The GTA will require that all Services within the scope of the CCOP solicitation meet the required security Service criteria. The current environment description above is not intended to provide a comprehensive list of desired security services, but is included to provide potential respondents with a general overview of what tools are currently used to enhance the State's security posture. The existing approach to security has been moderately successful in combating "IP centric" security threats, but no single set of standards has been adhered to throughout the State.

GTA believes that contact centers provide a significant opportunity to demonstrate and take advantage of converging technologies. GTA envisions that the State's contact centers will have integrated voice, data and video functionality for its interactions with the citizens the State. The Offeror is encouraged to develop contact center Services that will provide access to government's services via kiosk, today's Internet, video communications and traditional methods, such as calling via telephone.

Furthermore, it is not believed that these systems alone will meet the minimum-security requirements necessary for allowing State business to be conducted across a converged communication infrastructure in a manner that maintains the public's trust.

Functional Requirements

The Offeror's solution should support:

- Creative solutions for converged and integrated Services; meeting and exceeding the requirements as detailed in this SOW.
- Positioning the State to meet changing and evolving business and technical requirements, enabling the State to become a leader in providing advanced governmental services to its citizens.
- Structuring the best solution for the State: one that is structured to meet the State's business, technical, and economic requirements, and that will position the State to take advantage of emerging advances in technical services.

The provision of technical resources in support of GTA in the development of a clear, concise, strategic direction for Services.

Reasonable access to specialists as needed to assist GTA to develop and maintain the long-range Information Systems Plan and Equipment/Software Architecture Plan.

Immediate assumption on the Effective Date of operational support of the In-scope Services, Equipment, and Software, which includes but is not limited to: problem resolution, maintenance, upgrades, and configurations.

Assistance in technology planning, management, and special projects as requested by GTA and the VPAs.

Working cooperatively with Authorized Users, the State, and its architects and facility construction teams to facilitate effective communication, planning and implementation of the Services.

A secure, real-time network-accessible channel for Designated Users to access Services information (e.g., performance, orders, Install and MACs, capacity/performance management measurements, billing, etc.).

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide its overall approach to performing the cross functional Services described in the SOW. This includes but is not limited to: assisting GTA with decisions about technological changes and improvements, proposing alternatives that will be more cost effective for the State, continued automation of processes and functions, and improving the quality of Services.

The Offeror will describe its proposal for using emerging technologies and convergence opportunities to enable the State to reach its strategic objectives, increase operational efficiencies and enhance overall technology functionality.

The Offeror will describe how its solutions will utilize standards-based, integrated tool sets to move the State's environment from reactive to proactive monitoring and to enhance the stability and function of the environment.

Descriptions should clearly describe how the Offeror will meet the functional requirements or provide an alternative solution(s).

Help Desk

Desired Environment

GTA envisions the Offeror will transform current Help Desk operations through the deployment of Best Practice Customer Relationship Management (CRM) tools and methodologies that create a pervasive new culture focused around constituent service and delivering increasing value to constituents. The Offeror's CRM priorities should focus on delivering consistent, coordinated, event-oriented Services through multiple channels to CCOP constituents.

The Help Desk should be capable of supporting all functional areas of this SOW for all APA's; providing a single point of contact capable of; call handling (receipt and routing), and problem logging, tracking, resolution, root cause analysis, trending, and reporting.

The Offeror's call and problem management process must facilitate problem resolution in the shortest time possible. It must be flexible and facilitate a high degree of coordination/communication across groups, locations and regions. Clear problem ownership must be maintained throughout the resolution process, with progress updates communicated back to the Authorized Users.

The Offeror's approach to this responsibility will reflect a client service focus. In particular, Offeror will implement and maintain processes that encourage timely responses and end-to-end responsibility and ownership of each problem.

Functional Requirements

The Offeror's solution should support:

A single point of contact for calls for Services and other information technology functions, including calls for the State's Data Center and applications.

A first level Help Desk on a 7x24 basis and coordination with Authorized Users and points of escalation for all problem resolution activities when a solution cannot be achieved at the first level.

A single toll-free telephone number with adequate capacity for call volume.

A secure, network-accessible channel to the Help Desk information systems to allow Authorized Users to place requests.

Help Desk support may be provided at one or more Offeror locations that meet the following conditions:

Existing Offeror Help Desk centers may be located anywhere.

If creating a Help Desk center to support the State, the new center should be located within the State of Georgia.

Development and implementation, with GTA input and approval, of a formal plan for coordination of Services between APAs and Offeror and ensure its documentation in the Procedures Manual.

Acceptance of calls, requests for Services, and reports of problems from Authorized Users via multiple means (e.g., telephone, fax, secure, network-accessible channel, and e-mail). Provide assistance for Authorized User problems or requests, acting as the initial point-of-contact and coordinating problem resolution and request fulfillment.

Call and problem handling processes documented within a Policies and Procedures Manual.

Provision of a call and problem management tool that:

Is linked to a central database and an asset inventory system.

Can automatically page and send e-mails to appropriate support groups.

Provides call and problem exception reports in GTA-approved formats.

Is accessible via a secure network channel for record viewing and updating by Designated Users. Maintains Site histories and has the ability to automatically trigger notification to Help Desk staff of repeat problems by Site.

Can be accessed by Authorized Users through a secure, network-accessible channel to view status for the problems they have reported.

Includes security features so that only Designated Users can view, update, but not delete those records to which they have been assigned or to which they have been given authorization to access. Access rights and archiving record retention rules will be determined by the State.

Includes contact and location information for Authorized Users.

Is capable of associating assets with contacts and locations.

Is capable of automatic escalations based on problem category, severity level and solver group to assure the appropriate response as defined by the appropriate Service Level.

Supports the ability to designate certain Authorized Users as having a high priority.

Providing Designated Users licenses as necessary to access the call and problem tool.

Implementation of methodologies to prevent problem recurrence.

Performance of root cause analysis and make recommendations to fix root causes.

Conducting, at GTA's request, meetings to address Offeror's problem resolution activities in the event that there is a recurrent problem.

Development of escalation procedures with GTA's input and approval that would:

Include definitions of the elapsed time before a problem is escalated to the next levels of involvement (and notification) of various levels of Offeror and GTA management.

Automatically prioritize State-identified high-impact systems (as defined by GTA based on the potential impact the problem will have on the State's ability to fulfill its mission) and Equipment such that, when outages occur, they are treated with the highest priority and problems are escalated appropriately.

For all classes of problems, such escalation procedures should reflect:

The severity of the problem

The complexity of the environment.

Include provisions for progress updates to Designated Users after a problem ticket reaches a certain escalation level.

Immediate notification to Designated Users of system outages on critical systems, and providing progress updates as agreed to in the escalation procedures. Documentation of escalation processes is to be included in the Procedures Manual

Notification to Authorized Users and his/her APA initiating the call when an issue proves to be a non-resolvable problem and gaining concurrence from the GTA Project Executive (or its designee) that such problems cannot be resolved before closing such problems.

"Push" calls status back to the affected Authorized Users.

An on-line knowledge database to share Help Desk policies, procedures, tools, best practices and methods among APA personnel that is continuously updated and populated over the Term.

Coordinating tours of the Help Desk for Designated Users, provided that such tours will be reasonable in frequency and subject to reasonable prior notice.

An on-line Offeror problem call and problem management system training for Designated Users.

Taking appropriate action to communicate status of broad scope problems to Authorized Users upon receipt of notification from support groups of Services (e.g., status message, e-mail notification).

Proactive identification of trends in reported problems, and notification of appropriate support groups.

Processes for remote control access of distributed computing sessions and documentation of them in the Procedures Manual. Prior to session acquisition, provide for the Authorized User to provide permission to the Offeror Help Desk analyst for the session acquisition, using APA's-approved security procedures (i.e., screen prompt and verbal permission).

Provide persistent notification indicating remote session control of the desktop to the Authorized User's desktop monitor during the entire time the session is remotely controlled.

Log the Authorized User's consent to receive remote support, time and date remote control began, and duration.

Logs shall be provided at the APA's request, and shall be retained for a period of no less than 270 days.

Providing Designated Users up-to-date escalation lists of Offeror contacts for notification of problems associated with each of the Service areas on a secure, network-accessible channel.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will describe how it plans to implement tools, procedures and best practices in support of GTA's goal of delivering consistent, coordinated, event-oriented Services through multiple channels to CCOP constituents.

The Offeror will provide an overview for how it will operate a Single-Point-of-Contact, first level Help Desk for all Services that coordinates Authorized User support for the State, including call and problem logging, tracking, resolution, root cause analysis, and trending.

The Offeror will describe how it delivers these functions in environments similar to the State.

The Offeror will describe any software tools it will use to administer these functions.

The Offeror will describe how it will employ procedures for problem escalation; establish severity levels with the State and how it will implement measures to avoid recurrence of problems.

Descriptions should clearly describe how the Offeror will meet the functional requirements or provide an alternative solution(s).

The Offeror will describe the flexibility and availability of reports related to Help Desk activities

Change Management

The State desires the Offeror to provide a comprehensive and integrated approach to Change Management; including changes to any in-scope system or its components across all aspects of the Services environment. Changes usually vary in scope and impact to the environment, may be critical in nature, and will require varying levels of management. Change Management Services includes proactive management and implementation of planned changes for all Services through tools, processes and

procedures. The goal of Change Management is to eliminate or minimize negative or unforeseen impact to the State's Services environment.

Change Management includes those activities that support the State's business process re-engineering efforts.

Change Management includes procedures for managing emergency and other unplanned changes. The Offeror must be capable of supporting the State's responses to natural disasters, States of Emergency, and other declared emergencies.

Change Management includes supporting the State business case development initiatives. Change Management also includes efforts supporting continuous improvement. The State envisions the Offeror including continuous improvement of the processes, procedures, and technology used by the State.

It is expected that Change Management procedures will be developed with input and approval from the GTA and documented in the Procedures Manual.

Functional Requirements

The Offeror's solution should support:

Development of Change Management procedures, with input and approval from the GTA, which shall govern changes to the State environment with respect to the Services provided. The result of this effort should be a Procedures Manual.

Performing Change Management functions in accordance with the Procedures Manual.

Obtaining approval from GTA for any changes to Services prior to implementation.

Reviewing, scheduling and communicating all proposed Services changes with GTA and the affected APAs and all other service providers to minimize disruption of normal business processes.

Scheduling network outages related to installation and maintenance during Maintenance Windows.

An effective Change Management process that:

Facilitates coordination and communication across groups, Sites GTA and APAs.

Includes an impact assessment, back-out plan (with specific criteria associated to executing the back-out plan identified), end-to-end test plan where appropriate, and clear change acceptance criteria.

Maintains responsibility for individual changes throughout the process, with regular and appropriate progress updates communicated back to those affected.

Integrates changes across in-scope platforms and Sites.

Provides an interface to a problem management system.

Includes an audit trail of any and all changes to the production environment made according to the Change Management Procedures.

For emergency or urgent problem changes:

Implement such changes as are necessary and in a manner that is minimally disruptive.

In all but the most dire circumstances, a Designated User will be apprised of and approve the change prior to implementation.

In all cases, such changes will be reviewed with a Designated User within 24 hours of the change.

Integrates the Change Management process in an online manner into the automation strategy. The integration is to link:

The service procurement process to changes in the configuration database

To other change requests.

Link change requests to the Asset management process.

Includes a complete test plan.

Includes inside delivery of Equipment and/or components and coordination of such with Designated Users.

Provides for the Offeror to pay all shipping costs to and from Sites.

Includes a completed description of change requests including a description of the change, purpose and justification, risk analysis, schedule, implementation procedure, back-out procedure, and test plan.

Includes a comprehensive contingency plan for each change that presents a potentially high risk or high impact to the State's operations or business, including: back-out procedures, notification and escalation lists, work-around plans, affected resources, and risk assessments.

Provides for full support and maintenance for mobile Services on a depot basis that will include replacement equipment and salvage of data when necessary.

Collecting data by Service category on every change attempted, including the cause of any problems, measures taken to prevent recurrence, and whether the change was successful from the perspective of the user of the system. This data will be summarized and reported to APAs on a regular basis, at least monthly. Such reports should be provided to GTA upon request.

Scheduling outages by Site for system maintenance, expansions and modifications during hours that meet the APAs operational needs and minimize disruption as approved by the APA.

Communications with Designated Users that:

Include Designated Users as part of the change review, approval, and scheduling and communication process.

Submit proposed changes in advance to GTA and the affected APA, Designated Users, where appropriate following the Procedures Manual.

Provide a schedule of implementation dates to the affected APA for determination of any existing conflicts with business events.

Avoidance of any changes that:

Adversely affects the function or performance of, or decreases to any significant degree the resource efficiency of, the Services,

Increases GTA's costs or fees, or

Impacts the way in which GTA or any APA conducts its business or operations, without first obtaining GTA approval.

Negatively impacts Service Levels.

Acceptance test procedures, to be completed prior to implementing changes:

Develop acceptance test procedures for installation and changes to the Services, and for verifying restoration of availability following problems with network circuits or components, premise cabling, or Equipment.

New Services, circuits, or Equipment will not be deemed accepted until after Offeror has notified GTA and or the APA as appropriate, that the installation change or restoration has successfully passed Offeror's testing process (such notice will be provided within a reasonable time), and that GTA and or the APA has accepted such changes or restorations in writing.

Routine maintenance changes which:

Perform such changes during regular periods scheduled in advance and approved by APA.

At the GTA's or the APA's request and upon reasonable notice, provide for the Offeror being willing to change scheduled Maintenance Windows.

Give GTA and or the APA prior notice, according to the Procedures Manual, of the maintenance to be performed during scheduled Maintenance Windows.

In the event that there is a need for routine maintenance for emergency systems, provide GTA and the appropriate APA's with notice according to the Procedures Manual, and perform such maintenance to minimize interference with the business and operational needs of the State.

Systems will be unavailable during Maintenance Windows only to the extent necessary for systems' maintenance purposes.

Provision of regular reports on the status of scheduled changes.

Maintaining a comprehensive list of projects and dates.

On a regular basis, with scheduling to be agreed between GTA and the Offeror, conducting Change Management meetings with the GTA Project Executive or designee.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will manage and implement control changes to the State Services environment and how these processes will facilitate communication, ensure a tested back-out plan exists, and provide for a high degree of successful changes with minimized disruption to the State.

Provide an overview of how the Offeror can support the State's process improvement efforts. Include a description of the roles and responsibilities the Offeror is willing to take in support of process improvement.

Describe an overview of how the Offeror can support the State's initiatives for continuous improvement.

Describe how the Offeror intends to incorporate industry standards and best practices within the Change Management process.

The Offeror will describe its experience in managing complicated transitions in large, decentralized IT and telecommunications environments similar to the State.

The Offeror will describe its project management methodology including how it will provide detailed plans that will include timeframes, tasks, milestones, roles and responsibilities for State and Offeror personnel and any major task contingencies.

Problem Management

The State envisions a problem management process in which the Offeror assumes primary responsibility for the resolution of all problems encountered by Authorized

Users. Primary responsibility includes first point of contact for problems that are related to in-scope Services, but are not the contractual responsibility of the Offeror.

The State desires the Offeror to provide Problem Management methodology that involves identifying and classifying problems, determining escalation procedures and documenting all the information surrounding the characteristics and resolution of the inquiry. Every problem or request must be logged into a problem management system. All analysts who encounter a problem, regardless of their support tier, are responsible for documenting and forwarding the problem description and supporting data to the Help Desk for resolution. It is important to the State that the Offeror avoid prematurely closing problems and failing to log in incidents.

All problems should immediately be assigned a severity level according to the business risk and the potential impact of the problem. The GTA has provided a copy of desired Service Levels on the basis of severity level within the Service Level Section. To ensure that problems have a minimal impact on the enterprise, the Help Desk must prioritize problems, monitor problem status and assess the potential frequency of recurrences. For example, while a permanent-fix solution is being developed, enterprises should communicate within the organization to ensure effective bypass and recovery procedures

The Offeror should take a leadership role in the problem management process by being responsible for the following activities:

Funneling problems to the appropriate organizations for resolution;

Monitoring the status of outstanding problems; and

Enforcing schedules for timeliness of problem resolution.

Problem management is expected to proactively avoid or minimize disruption to Services and to promote timely repair/restoration.

Functional Requirements

The Offeror's solution should support:

Coordination and integration of the problem management process with the call/problem management tool used by the Help Desk.

Implementation of mutually agreed policies and procedures to accelerate and improve the problem management process.

Maintenance of a mutually agreed emergency contact list and escalation procedures to report and resolve problems.

Assessment of the impact of problems on Authorized Users and APA's, and report assessment to both the affected Authorized User, and APA.

Immediate notification to APAs GTA of any problems that might affect availability of Services.

Verification of the restoration of Service, Equipment, and Software availability following problems.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will perform proactive production monitoring, problem management, including problem diagnosis and resolution, for all Services, and for all Equipment and Software.

The Offeror will describe its procedures that ensure real time updates of moves, adds and changes to provide the latest customer information to its support personnel.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

Record Archival

Record Archival services include the electronic recording or copying and verification of information, configuration and data files onto media that can be secured away from the environment and used in future recovery processes.

Functional Requirements

The Offeror's solution should support:

Archival of records such as billing, Service Level records, project documentation and other Services related records as deemed necessary by GTA.

Restoration from any Software failures resulting in loss of data being restored using data that has aged no longer than the previous day's recovery data backup.

Measures necessary to protect the integrity and confidentiality of the backup data.

Provision of recommendations to GTA regarding backup and recovery considerations, such as improved levels of protection, efficiencies and cost reductions.

Assisting APA's and their Authorized Users in lost or damaged file recovery from Server backups.

Performance of recovery procedures in response to security violations that result in lost/damaged information.

Periodic testing of procedures to ensure viability of the process.

Off-site data storage, including:

Retrieval and return of off-site stored data;

Performance of off-site vaulting of data media; and

Maintenance of a catalog listing off-site content.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will address and perform the APAs' record archival requirements, which includes storage of backup media, and processes for recovering data from backup media, and periodic testing to ensure process integrity.

Performance, Capacity and Configuration Management

GTA envisions performance, capacity and configuration management including such areas as capacity planning, workload profiles and measurements, traffic analysis and forecasting, long-term capacity planning, and diagnostic toolsets for CPU usage. Additionally covered are software resources and distribution management, resource databases, integrated network analyzers; application development system monitors; etc.

In addition, it is imperative the Offeror manage the performance, capacity and configuration of the State's systems such that APAs are not subjected to crises and potential resultant Service degradation caused by unexpected growth.

Functional Requirements

The Offeror's solution should support:

Capacity management efforts that include:

- **Prepare semiannual growth projections and present the results in a formal capacity plan.**
- **Installation and support of sufficient capacity of all In-scope elements to meet the business requirements of the State.**
- **Utilization of capacity planning models and methodologies and incorporate GTA's capacity planning recommendations into its planning model.**
- **Formally reviewing capacity requirements as part of GTA's normal business planning cycle.**
- **On an annual basis at a minimum (within 30 days prior to the Agreement anniversary date), delivering to GTA forecasts of systems/Services requirements in response to growth projections provided by GTA.**
- **Validating capacity forecasts against actual utilization.**
- **At least quarterly, revising the capacity planning model based on actual performance and providing this model to GTA.**
- **Assistance with analyzing application capacity and performance impacts to Services and systems, and providing technical advice and support to the business applications and DBA staffs, as required.**

Performance management that includes:

- **Performance of those activities required to continuously evaluate the principal performance indicators of all Services operations, and identify actual and potential bottlenecks.**
- **Establishing and reporting on network trends for decision making and planning. These measurements may include but are not limited to: overall throughput, percent utilization, error rates, and latency or specific performance measurements such as packets per second.**
- **Implementing performance management and monitoring tools to be used in conjunction with the Help Desk problem/call management system and the Asset management database.**
- **Optimizing the Services in terms of cost effectiveness and efficiency, but without sacrificing performance.**

Providing measurements of both peak and average levels to the State.

Providing GTA access to secure on-line, real-time network performance monitoring for all Services delivered to APA's.

On a monthly basis, providing GTA reports showing the performance results of supported systems (e.g., disk, processor, memory, bandwidth utilization, etc.) performance, utilization, and efficiency.

Management and monitoring of all performance and system resources and identification of trends that may adversely impact Services performance. Proactive management of network congestion such that all subscriptions are not violated due to third party competition for network resources.

Configuration management that includes:

Establishing standard configurations for Equipment with GTA and VPA approval.

Maintenance of a library of information and documentation for any existing, new, enhanced or modified system (e.g., initial purchases, upgrades, patches, etc.) installed in the environments of the APA's for all Equipment.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide its approach to providing and conducting performance/capacity planning and management for all Services. This includes monitoring, evaluating and reporting on the performance of all Service areas.

The Offeror will propose a variety of metrics, indicators and measurements that will allow GTA to accurately gauge the real-time performance of the Services, and to predict the long-term growth of the Services.

Offeror will provide performance measurements that will allow for the independent validation of all Service Levels. Offeror will describe how the performance measurements will be validated.

The Offeror will also describe how it will provide configuration management for all system arrangements. Identify what areas of Services will be affected by unanticipated changes in demands on capacity.

The Offeror will describe the life cycle of their system(s) as well as how it intends to remain current following full implementation.

Services Monitoring

Services monitoring includes those activities related to the Services that check on, watch, keep track of or warn of conditions or events by electronic means that are either inside or outside of established operating parameters.

Functional Requirements

The Offeror's solution should support

Provision of Services monitoring and be consistent with the high level of quality expected of a first tier global provider of managed network services.

Providing Designated Users with a secure, network-accessible channel with a read-only view into the network maps, trouble ticketing system and performance management systems as befits their duties and responsibilities.

Assuming responsibility for all console operations, including monitoring all processing within the State's LAN/WAN and In-scope Server environment, alarm systems, environmental controls, and transmission and reception of polling information from outside organizations.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how Services' performance will be monitored and maintained across the State, including how the Offeror will monitor and react to system alarm and environmental malfunctions.

The Offeror will describe how tracking and monitoring of Services and systems will be provided on a real-time or near real-time 7X24 basis, and how these monitoring activities and information will be available to Designated Users via a secure, network-accessible channel.

The Offeror will describe the automation of console functions and any processes or procedures to be used, and how the reception and transmission of polling information from outside organizations is to be performed.

The Offeror will describe how it will provide for GTA and VPAs to observe or query the Services' monitoring network management system.

Security Services

This section covers the prevention of security-related problems, including threats to State information, unauthorized access to State information services, and maintaining confidentiality of sensitive information. Security Services include end-to-end management of the environments procured and covered by the RFP and associated

contracts. Security management should cover the gamut from monitoring and detection to incident response.

As part of the security Services, the Offeror will assist GTA and VPAs in developing security policies that take into account the diverse characteristics associated with the unique business requirements of each entity's core functions.

The proper implementation of an information security program for safeguarding the State's information as it resides on a converged infrastructure is a top priority.

These Security requirements apply to all Services in this SOW.

The State of Georgia plans on adopting the ISO 17799 Code of Practice for its information security management standard. All Offeror proposed practices and solutions should be compliant with this framework. The ISO 17799 standard can be obtained at: http://www.iso-17799-security-world.co.uk/what.htm

GTA, VPAs and the Offeror will discuss the range of security tool options and GTA will have final approval of the security tools to be used.

Functional Requirements

The Offeror's solution should support:

Management and operation of authorization control systems to State systems and information.

Prevention. The Offeror should:

Be responsible for implementing and maintaining the effectiveness and currency of intrusion detection systems and encryption methods used to protect the State's data.

Ensure that the Offeror and agents of the Offeror will be pre-authorized and have appropriate access prior to entering State Sites. This may include badges, the use of State escorts, and other methods of access.

Cooperate with the State in assessing compliance with State security policies of Offeror-provided tools and systems.

Install, update and maintain security Software, identify and analyze system security problems, maintain network access authority, process approved security requests, perform security audits, provide incident investigation support, and provide Application security support and consulting.

With appropriate GTA approval, develop and document all necessary security procedures and breach of security action plans and submit them to GTA for review, approval and possible inclusion in the Procedures Manual.

At the level appropriate for Offeror's performance of day-to-day security functions, consult with GTA to identify security

risks and recommend and implement, subject to GTA approval, procedures to minimize such risks.

Assist the State in developing APA-specific security policies that take into account the diverse characteristics associated with the unique business requirements of each APA's core functions.

Upon publication or when notified by the State of new vulnerabilities or exploits, follow best practices to correct deficiencies (e.g., applying recommended software patches, updating virus definitions, updating intrusion detection signatures, hardware configuration, etc.).

Provide the capability to monitor in-bound network traffic and internal LAN traffic for intrusion attempts and violations of established security procedures.

Conduct personnel security investigations (i.e., background checks) on all Offeror employees and contractors who will have access to critical components of State Services (e.g., administrator access, software/hardware Install and MAC, physical network components, monitoring services, etc.). Refer to Section 6.2.32.

Identify and prevent unauthorized connections to State networks and Services resources through modems and other external connections.

Identify and install all relevant security patches to installed software.

Upgrade Services components necessary to support emerging security standards as they develop in a timely manner.

In the event GTA elects to explore and/or implement Public Key Infrastructure technologies (PKI), security applications or Services using encryption technology must be compliant with those standards.

Provide at least the minimum network security requirements as outlined by applicable federal information security guidelines and policies. This applies only to locations specified by Designated Users that are under such jurisdiction, or optionally elect to subscribe to such level of protection. The current federal guidelines can be found in the Regulations Section 6.2.25 within the Cross Functional Services Requirements.

Provide data protection on all connections and file transfers between Authorized User Workstations and Internet Servers

in accordance with the State's information security standards.

Deterrence. The Offeror should:

Be responsible for implementing and maintaining the effectiveness and currency of encryption systems.

Take reasonable and appropriate action designed to prevent unauthorized access to the State environment, in accordance with State requirements

Establish and maintain safeguards against unauthorized access, destruction, loss or alteration of State data in the possession of Offeror that are no less rigorous than the most rigorous practices actually performed by the State.

Adhere to APA specific security policies and practices, to include access to buildings, documents and information left on the desktop, and information on State computers and monitors.

Detection. The Offeror should:

Perform, or assist in performing, security audits as set forth in the Agreement.

Establish and administer violation and access attempts reporting mechanisms.

Report all attempts at illicit monitoring, interception, or eavesdropping to GTA to the extent known by the Offeror.

Promptly provide written confidential reports of security breaches discovered or made known to the Offeror.

Prepare and retain documentation of breach of security incidents and provide copies to GTA at a frequency to be agreed upon by both parties.

Upon detecting an active or suspected security event:

Immediately notify GTA and the appropriate APA(s) about such events.

Provide details of resolution efforts to GTA and the appropriate APA(s).

Provide information about State and/or Offeror resources affected or potentially affected by the security event.

Response. The Offeror should:

Eliminate causes of security events, and their effects, and restore affected systems and services to their status before the security events, including recovery of information that is lost/damaged from the most recent trusted/clean backup.

Submit a procedure for initiating isolation of Services to eliminate the cause of security incidents, including where appropriate, shutting down the Services to prevent further unauthorized access, and restoring affected systems and Services to their status prior to incidents.

As it pertains to the In-scope Equipment, recover, or attempt to recover, from the most recent backup or by using forensic methods to extract data from the device as required, information that is lost or damaged as a result of a security violation.

Minimize the time between a security event occurring and its detection.

Provide incident investigation support to GTA and the appropriate APA(s) when requested.

Other security functions. The Offeror should:

Offer the same or greater level of security protection consistent with industry standards or best practices as necessary to satisfy the business and operational requirements identified by the State.

Be jointly responsible with GTA for the selection of the standardized interfaces for security Services to ensure Offeror-State and Intra-State interoperability.

Cooperate with and coordinate Offeror's security activities with current service providers of legacy services.

Implement security provisions as contained in the Procedures Manual as they are developed or accepted by GTA and other recognized governing bodies whenever appropriate.

Ensure the strict confidentiality of State data and make all necessary provisions to protect State data from unauthorized viewing, tampering, or distribution to individuals or entities not expressly authorized by the State to access State data.

Process State-approved/completed security requests.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will describe how its approach will include an overview for its approach to security by proposing a security policy for a generic organization, and outline how it will propose to implement security solutions for the State based on the developed model.

The Offeror's approach to security will include assuming the current environment as well as cooperating with GTA to define and implement emerging information security initiatives.

The Offeror will also describe how it will implement an information security approach that follows a service model concept for security, including identification, access, authorization, and auditing.

The Offeror will describe its experience protecting sensitive and confidential information in providing IT or telecommunications Services to either the public or private sector in environments similar to the State.

The Offeror will detail specifically to what degree they the Offeror will agree to be responsible for data security throughout the Services to be provided.

The Offeror will describe any software tools it will use to administer these functions.

The Offeror will describe its approach to each of the following security areas:

Authentication**: The means used to establish with some acceptable level of assurance, the identity of the Authorized User, Equipment, or other entity in a computer system, often as a prerequisite to allowing authorized access to resources in a system.**

Authorization: **The level of permission an Authorized User or Designated User or process has to use a computer or information resource. Authorization is the technical means to enforce permissions - controlling what information or applications an Authorized User can use or run, and the modifications they are allowed to make.**

Data Integrity: **An attribute of data relating to the preservation of (i) its meaning and completeness, (ii) the consistency of its representation, and (iii) its correspondence to what it represents. Data integrity provides evidence or assurance that data has not been altered in any fashion - intentionally or otherwise - particularly in storage or transmission.**

Confidentiality**: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes, assuring that only the intended parties can read a particular piece of information or data.**

Accountability: **The means to ensure that other security Services are being employed correctly. This includes the ability to identify, verify, and trace system entities as well as changes in their status in such a way that ensures that the actions of an entity may be traced uniquely to the entity. Alerts should be triggered by failed or successful intrusion attempts or by the unusual state of a service or performance metric.**

Availability/Reliability: **Assurance that information and communications Services will be accessible, ready for use and operating according to specification when expected by an Authorized User.**

Non-Repudiation**: The characteristic that proves, without reasonable doubt, an individual or entity performed a particular transaction.**

The Offeror will also describe how it will implement an integrated information security approach that follows a service model concept for security throughout the enterprise (e.g., network, hosts, and In-scope Software), that addresses the four aspects of security: prevention, deterrence, detection and response.

The Offeror will describe the life cycle of their system(s) as well as how it intends to remain current following full implementation.

Quick Response

The responsibility for quick response varies throughout the APAs. Each APA may or may not have a quick response plan. The Offeror will be required to develop, document and maintain a statewide quick response plan that provides for the deployment of temporary Services within the time frames established as required to meet the quick response requirements of the State.

The Offeror is to become responsible for providing temporary Services in response to a Quick Response request by the GTA.

There are two categories of quick response requirements:

- Disasters in which Equipment and Services supporting Authorized Users are damaged or impaired (e.g., hurricanes, floods, fires, building collapses).
- Emergency situations in which no Equipment is damaged or impaired, but Authorized Users require additional Services to provide support to citizens impacted by disasters (e.g., an agency may augment local staff to assist in disaster recovery operations. The augmented staff may require additional Services).

Both categories may occur anywhere within the State of Georgia. They will be of limited duration until the situation is resolved and/or permanent Equipment and Services are installed. In both instances, Designated Users will identify when a quick response

situation occurs, provide the request to GTA who will then forward the request to the Offeror.

Functional Requirements

At a minimum, The Offeror's solution should support:

The ability to provide at least one hundred (100) wired or wireless devices with connectivity including domestic long distance within twenty-four (24) clock hours of notification of a quick response situation.

Configuration of lines to direct incoming calls to a single listed number accessible by all telephone sets (e.g., the lines may be in a hunt group).

The ability to provide additional local service telephone lines including domestic long distance within forty-eight (48) clock hours of notification of a quick response situation. These additional Services must be integrated into those listed in Item 1 above.

Installation and maintenance of Data Communications connections sized as specified by the State (Full Service or Transmission Circuits) within twenty-four (24) clock hours of notification of a quick response situation.

Workstations, printers, and Servers. The Offeror should:

Be able to provide up to twenty-five (25) networked Workstations equivalently equipped with the current Seat bundle and loaded with the Standard Workstation Software within twenty-four (24) clock hours of notification of a quick response situation.

Be able to provide up to two (2) networked printers within twenty-four (24) clock hours of notification of a quick response situation.

Be able to provide additional networked Workstations and networked printers as described above in Item 5.a and 5.b within forty-eight (48) clock hours of notification of a quick response situation.

Be able to provide additional networked peripherals as necessary within forty-eight (48) clock hours of notification of a quick response situation.

Provision of mobile radio communications and video broadcast services sufficient to support the Georgia Emergency Management Agency requirement to provide on-the-scene coordination of state emergency communications during an emergency disaster.

The ability to provide on-the-scene Two Way Radio communications, within twenty four (24) clock hours upon notification, for a minimum of 300 users between State, local and federal agencies in the event the Two

Way Radio infrastructure is inoperative or additional Two Way Radio communications are required at the emergency location.

Provision of adequate power for deployed Equipment and Services supporting a quick response requirement.

Providing daily reports beginning the first day after notification until GTA and or the State terminates the Quick Response situation. Reports should include information on the Equipment and Services provided their quantities, the deployed locations, and any problem areas.

Immediate availability of IVR systems to support information dissemination to the calling public.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will respond to situations requiring a quick response, including how it will provide and support Equipment and Services.

The Offeror will provide an overview for how it will monitor Equipment and Services to ensure the State is able to meet the needs of the State's citizens.

The Offeror will provide an overview for its disaster recovery plan and what interaction between itself and the State is necessary in order to fulfill all Service Level requirements.

The Offeror will provide an overview for how it will initiate its disaster recovery plan to restore affected entities according to the Georgia Emergency Management Authority (GEMA) priority scheme.

The Offeror will provide an overview for all instances of planned 'zero-time' recoveries for voice services, in which the Offeror will provide either an automated fail-over facility or a loaner pool.

The Offeror will be required to meet Service Levels at all times, regardless of circumstances whether man-made or acts of God. For this reason, the Offeror should propose an infrastructure design that incorporates strategies such as minimum single points of failure, redundant geographically diverse facilities, fault tolerant network designs, and other disaster recovery high availability practices.

Making changes to these requirements as GEMA's and GTA's quick response plans change throughout the Term.

Disaster Resistance

The Offeror will be providing Services upon which the law enforcement, emergency management systems, health care, and emergency response systems rely. As a result,

the Offeror will be required to meet a higher guarantee of availability and all other Service Levels for identified critical Sites. Downtime, even minutes for a high-availability system, can represent a serious business interruption that may result in human casualty. The primary mission of these critical Sites is to provide public services necessary for the protection of life, maintaining civil order, and responding to natural disasters.

Services for the listed critical Sites must be maintained at the levels specified in the SLA's regardless of circumstances such as natural disasters, civil unrest, information system attacks, and other unforeseen events.

GTA envisions the Offeror proactively participating in Business Continuity Planning (BCP) as well as assuming responsibility for the execution of tactical and operational plans required to support the strategic BCP plan.

The Offeror must provide continuity services that help APA's maintain critical business continuity and recovery functions in an emergency. Services must reflect the need for customized continuous availability, rapid recovery, and hot-site recovery. BCP will include planning and action taken in preparation of potential acts of terrorism, unpredictable natural disasters, infrastructure failures, or unexpected downtime with hardware or software.

Functional Requirements

The Offeror's solution should support:

Design of an infrastructure that provides for the maximum availability and performance commercially available for all services utilized at each critical Site.

For standby Equipment that will be used, switchover must not require manual intervention to restore service and should have minimum switchover time commercially available.

The ability to, on a Site-by-Site basis, specify any backup power requirements necessary for deployed premise equipment. At the State's sole discretion, the Offeror will provide and coordinate with the affected Site's Designated Users and its building owners for the installation of any backup power needed to support the Offeror's premise equipment.

Coordination with the State to provide building modifications, lighting, space, physical security and environmental requirements necessary to fulfill the disaster resistance requirement.

Accept responsibility for participation in BCP for the State's enterprise network.

Accept responsibility for BCP for the Services provided to APAs.

Annually conduct risk analysis to determine the enterprise's ability to recover business operations based on a complete destruction of the production facilities. Provide a gap analysis report will result, identifying where recovery plans do not support current business operations.

Establish a crisis management team and participate in the State's crisis management team.

Establish an emergency decision-making hierarchy to address the potential that some executives may be unavailable.

Be prepared to make regular and updated declarations of the steps the enterprise is taking to deal with the crisis.

Update personnel contact lists and calling trees, including multiple forms of contact information — e.g., office, home, mobile and vacation home telephone numbers, pager numbers, and office and personal e-mail addresses.

Establish a personal tracking procedure so that the location of personnel is known at all times during normal business operations.

Establish a personnel awareness program — i.e., a program educating personnel to potential disasters — and train personnel to react

appropriately during an event, including evacuation and contact procedures.

Determine other methods of communication besides telephone service to establish key communications. E-mail, instant messaging and the enterprise's Web site can be used for communicating with personnel. Personal response systems can be used for limited-distance communications for on-site staff, or for those in close proximity.

Set up a toll-free telephone number that personnel and their loved ones can use to receive and disseminate information.

Obtain alternate office space to be used during a disaster — e.g., at an alternate company facility, from a disaster recovery service provider, at a hotel or through an industry association. The use of a "buddy site" (i.e., facilities at an industry peer's business location) may not be available as it may be experiencing similar problems. Although disaster recovery service providers have offered office space and equipment to non-customers during crisis events, they can't similarly offer recovery services for an enterprise's IT infrastructure.

Adhere to State standards regarding extra expense and business interruption insurance policies to assure the State that the Offeror is capable of funding BCP scenarios of business operations.

Adhere to State standards regarding backup schedule and media storage strategy to ensure that the entire information flow, including applications, connectivity and access endpoints, can be recovered, and the backup media can be easily recovered and brought to the alternate recovery site.

Making changes to these requirements as GEMA's and GTA's disaster resistance plans change throughout the Term.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will describe its plan for disaster resistant strategies (e.g., minimizing the number of single points of failure, diverse communication media types and technologies, redundant geographically diverse operations facilities, fault tolerant network designs, diverse routing, etc.).

The Offeror will explain how Authorized Users will be involved in developing and testing the disaster recovery plan.

The Offeror will also describe how it will initiate its plan to restore affected entities according to the Georgia Emergency Management Authority (GEMA) priority scheme, should a multiple site outage be realized.

The Offeror will describe its commitment to supporting the Business Continuity Planning requirements of the APAs. Including, strategic planning, tactical and operational planning, tactical and operational execution.

Describe any limits the Offeror's anticipates regarding extra expenses incurred as a result of the execution of BCP activities.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will explain the implications of responding to requests for disaster recovery.

Order Fulfillment

GTA describes order fulfillment as a group of activities including the solution design, qualification, satisfactory delivery, installation, and setup of products and Services.

Currently, the products and Services procured by the State are ordered in many different ways. The orders placed with GTA and those placed directly to other vendors and suppliers primarily with a Purchase Order document are inconsistent and varied based on the product and Service.

It is the desire of GTA to greatly simplify the order fulfillment process for In-scope products and Services. The simplification of packaging, ordering, and delivery of the products and Services can accomplish this for all customers.

At a minimum, the order fulfillment activities GTA requires are:

- Design and selection assistance for In-scope products and Services.
- The provision of a service order module and database on a secure network-accessible channel for order requests of products and Services.
- An on-line Services catalog with prices accessible to Designated Users within the service order module and also accessible independently of the service order module.

Coordination of In-scope product and Services deliveries within predetermined time frames with verification of satisfactory delivery.

GTA will continue to use the Purchase Order document where applicable but will also use the service order module provided by the selected Offeror for ordering many Services and products.

GTA desires an order fulfillment process providing an integrated electronic system for all order channels, including current PO channels, Internet Web channels, etc. GTA anticipates the need for the Offeror to transform the current processes to link all channels into the fulfillment systems.

Functional Requirements

GTA will retain responsibility for approving MPA orders prior to placement. GTA will also retain responsibility for approving additions to the products and Services catalog provided to all APAs. No additions can be made to the products and Services catalog without prior GTA approval. BOR will retain responsibility for approving University system orders prior to placement. Political Subdivisions will retain responsibility for approving their own orders according to their own procedures prior to placement.

All APAs will send their orders for products and Services to Offeror through the GTA in accordance with the Procedures Manual.

The Offeror's solution should support:

The provision and maintenance of an approved Catalog of the standard products and Services including current prices.

Verification that appropriate GTA approvals have been obtained prior to placing order.

A process whereby the Offeror will only accept, process, and place orders that have been approved by GTA and that are in the current GTA-approved catalog.

A service order module on a secure network-accessible channel that will:

Allow Designated Users to access the service order module for entry of orders for products and Services.

Provide full product and Service options for orders at the APA level.

Provide options for orders for all Seat Services and Seat/Bundle options for an individual Authorized User.

Provide for ordering multiple Seat Services or Bundled options in one order.

Allow Designated Users to order Bundled Services as defined in the Catalog.

Provide a customized interface to State systems (e.g. PeopleSoft procurement/human resources) or other systems using provided API's, to be used after orders are approved and are ready for processing for orders entered through the online service order module.

Allow for an alternative order entry method by the acceptance of a customized interface from the State systems (e.g. PeopleSoft procurement) or other systems using provided API's when an approved purchase order is created by the State.

Include, at a minimum, the following information for each order:

Order number.

Date of the order.

"Bill To" and "Ship To" identifications and addresses.

State Account identification if different from the "Bill To" identification.

State Site identification.

Delivery dates and dates of performance of required preparatory services.

Complete list of the Services and product items covered by the order; including the quantity, model number, catalog name or identification number, and description.

The charge for each Service or product item.

Shipping instructions if applicable.

Location to which the products will be delivered and installed.

Scheduled installation date, not to exceed the maximum SLA intervals for the requested Service or product.

Primary and secondary Authorized User Site contacts with appropriate telephone numbers and e-mail addresses for each.

Accounting information appropriately for the APA's.

State Project identification if applicable.

Installations:

Deliver Services and/or products to APA's designated location(s).

Perform required preparatory services on or before the dates specified by GTA, and or APAs as applicable.

Products and Services will not be considered installed until the products and Services operate in accordance with its documentation and GTA guidelines.

Order terms:

Acknowledge receipt according to Designated User preferences (phone, writing or electronic) of each order within one business day.

Procure the product items and provide related Services, unless Offeror notifies GTA of reasonable objections to the requirements of such order in writing within two (2) business days of the receipt of such order.

Order changes: If a Designated User cancels or withdraws an order for any catalog Service or product after shipment, and Offeror cannot reasonably avoid the change or cancellation, Offeror may invoice the appropriate APA for out-of-pocket costs and reasonably related administrative expenses.

Order tracking to include:

Verification of the technical integrity of the order.

Verification of a proper GTA approval for the order.

Follow through on delivery, installation and final invoicing.

Allow Designated Users to review the status of outstanding requests for orders by access to an electronic order tracking system.

Allow Designated Users to access the service order module for review and approval update of orders.

Provide an alternative method (other than web access) for Designated Users to check order status and complete order entry.

Include a provision for an order change at no charge if an item is out of stock, back-ordered or has a long lead-time for delivery.

Invoices:

Process invoices from Managed Third Parties within 30 days.

Verify charges are appropriate for each State Site.

Include charges in approved billing methodology as defined in the Billing section to the State.

Returns:

In the event an APA returns any product following receipt, Offeror will take all reasonable steps to mitigate costs that might result from such returns, including leveraging the State's and Offeror's buying power to eliminate or reduce restocking fees and return freight charges.

Any unmitigated cost incurred by the Offeror will be invoiced to the APA with prior agreement by GTA.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror should describe how it would provide and support order fulfillment activities for Services and In-scope products to include the functional requirements detailed above.

The Offeror should fully describe the order module format and access, the product catalog format and access, and all product and Services delivery and installation processes.

The description should include how the Offeror proposes simplification of the order fulfillment activities and how orders for products and Services provided by the Offeror's subcontractors will be incorporated into the Offeror's order module and format.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

Billing

For purposes of this billing section GTA has identified three specifc categories of procuring agencies: MPA's, BOR (and its units), and VPA's

other than BOR.. Billing and reporting requirements related to billings will differ slightly for each category.

Currently, GTA bills these agencies for many telecommunications products and services delivered by GTA and for many products and services delivered by third parties (e.g., long distance service). Currently, all call detail information is provided directly by the carriers. The agencies are also billed separately by each vendor for each product and service procured independently from GTA such as cellular phone service, nation-wide pagers, radio maintenance, and distributed computing support as applicable.

With the implementation of this contract, GTA will transition from the role of supplier to that of "contract administrator". It is the desire of GTA to greatly simplify all related processes and to reduce the time currently required for bill interpretation and reconciliation. The simplification of packaging, ordering, and delivery of the In-scope products and Services, thereby simplifying the billing requirements can accomplish this for all customers. It is also the desire of GTA to have a very simple format for the bills created by the Offeror.

GTA envisions the use of a billing system that is capable of billing APAs for Seats, Bundles, other products and Services; pass through elements (if any), and administration fees that reflect the unique Services obtained by each APA.

It is the desire of the GTA that the Offeror include on each bill to APAs, administrative fees billed on behalf of GTA as defined in the Agreement.

Functional Requirements

At a minimum, the Offeror's solution should support:

A service that allows MPAs, BOR, and other VPAs to provide special account coding information that would be reflected on their respective bills. It will be the responsibility of those same entities to provide their unique information and updates with reasonable lead times for changes to this information.

Bills (invoices) sent directly to the MPAs, BOR, and other VPAs for Services and products on a monthly basis in the month following the billing period (i.e., July products and Services should be billed in August).

Bills that are accessible to Designated Users from a secure network-accessible channel in a format allowing the APAs to distribute or print the bill in total or by each "Bill To" account and in a format to allow download functionality to spreadsheet software such as MS Excel.

A separate detail on the bill of the administrative fees billed on behalf of GTA.

A designated Offeror lock box for the MPAs, BOR, and other VPAs to make payments on a monthly basis to the Offeror.

Payments from the Offeror to GTA transferred immediately to a designated GTA account for additional funds billed on behalf of GTA for administrative fees paid by MPAs, BOR and its units, and other VPAs.

Billing reconciliation assistance to Designated Users.

Billing for international calls.

Bills to MPAs:

One bill each month to each MPA in electronic format, suitable for interface into the State's accounts payable system using provided API's.

Summary total amounts for each MPA "Bill To" account detailing "Ship To" information.

Summary totals of all other unique accounting data for the "Bill To" account.

Details on the bill to include the number of Seats by Seat billed to the account.

Details by catalog item products and Services provided on a recurring basis and products and Services ordered, installed, and delivered during the billing period.

Call details for any itemized billing that is not flat rate such as international long-distance as specified in the Voice Reporting section of the Statement of Work.

Reports:

Reports available to each APA individually detailing or summarizing services by account and accounting information.

Reports available to GTA summarizing or detailing all Services for all APAs collectively.

Bills to BOR and its units:

One bill each month to BOR and each of its units in electronic format suitable for interface into the BOR's accounts payable system using provided API's.

Totals by BOR unit designated by BOR as a "Bill To" account.

Subtotals within each BOR "Bill To" account at departmental designations provided by BOR.

Detail billing to include an itemization of billed services such as a detail listing of the Catalog item, products or Services provided on a recurring basis and products or Services

ordered and delivered during the billing period including "Ship To" information.

Call details for any itemized billing that is not flat rate such as international long-distance (including authorization codes) as specified in the Voice Reporting section of the Statement of Work.

Reports:

Reports available to GTA, BOR and its units individually detailing or summarizing Services by "Bill To" account and sub-level accounting information.

Reports available to GTA, BOR and its units summarizing or detailing all Services for all BOR and its units as a whole.

Bills for VPA other than BOR and its units:

One bill each month in either electronic or paper format based on the request of each such VPA.

Summary by total amount for each such VPA's "Bill To" account detailing "Ship To" information.

Summary totals of all other unique accounting information for the "Bill To" account.

Details of the products and Services billed to the account. Include a detail listing of the Catalog item Services or products provided on a recurring basis and products and Services ordered and delivered during the billing period.

Call details for any itemized billing that is not flat rate such as international long-distance (including authorization codes) as specified in the Voice Reporting section of the Statement of Work.

Summaries by "Bill To" account identification.

Reports available to GTA and each such VPA individually, detailing or summarizing services by account and accounting information.

Offeror Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror should provide a complete description of its billing approach to APA's to include the functional requirements detailed above. The description should include how the Offeror will provide electronic bills and the on-line and download access to those electronic bills, the

option to have electronic interfaces to open systems' accounts payable systems, and reporting and billing reconciliation procedures.

The Offeror's description should include specific format examples for all components of the bills and a description of how invoices from the Offeror's subcontractors will be included in the same simple format on the same bill.

The Offeror should describe its terms for payments due, which should include credits, pro-rations, refunds and amounts in dispute if applicable.

The Offeror will describe the flexibilities provided in its billing system.

The Offeror will describe its experience in delivering these functions in environments similar to the State, particularly government related experience.

The Offeror will describe their approach to billing international calls.

Authorized User Training and Education

GTA values training as a vehicle to maximizing the State taxpayer's investment in technology.

Instruction to users on how to use products and Services when necessary is desired for multiple groups such as:

- Authorized Users.
- Designated Users.
- Smart buyers/State subject matter experts (e.g., tools, technology briefings, Offeror conferences, etc.) are responsible to act as technical interface between Designated Users/Authorized Users and the selected Offeror. GTA Smart Buyers are "Governance Custodians" of all In-scope Services, and must ensure the selected Offeror's technical and price solutions remain current and remain in the best interest of the State.
- Executives (e.g., industry briefing, Offeror conference, etc.).
- Special groups (e.g., call center supervisor/agent, IVR, CTI, adaptive Equipment users, State entities requesting education or skills assessments, etc.)
- Interface programmers.

Functional Requirements

GTA will approve all course content and delivery methodology and will ensure training is accessible as required by State and federal laws and practices.

Modifications to training program content will be reviewed and approved by the GTA's "smart buyers" prior to integration to the curriculum.

Interactive training programs will be reviewed and approved by GTA

The Offeror's solution should support:

Presentation of a comprehensive curriculum of training programs for all products and Services as required, using a variety of teaching modalities (e.g., one-to-one, small group, train-the-trainer, hands-on off site instructor lead, distance learning, on-line/CD Rom, group training, lab simulations, test environment management, etc.) for Authorized Users and Designated Users.

Reviewing and modifying course offerings at least annually during the Term.

Providing, on a secure, network-accessible channel, viewable and printable course descriptions that include at a minimum: course title, length of training, technology type, pre-requisite skills, course outline of goals and measurable objectives for skill mastery, methodology for presentation, post training competency expectations, and testing methodologies used (if any).

Provision of course development to the State's training agencies whenever possible.

Performing scheduling and registration services for courses.

Facilities and Logistics, The Offeror should:

Coordinate training facilities logistics with the State for on-Site training.

Propose methods to coordinate and use the State's training facilities for Offeror-led courses.

Develop a skills assessment tool for each course as required.

Ensuring that attendance reports will be made available to the State.

Electronic registration reports that would include course, student, date of attendance, status (complete/cancelled/competency measure not met), agency, division, student primary telephone number, and student identification number.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will ensure Authorized Users and Designated Users will be educated to the operation of technology solutions covered by this RFP as requested by APAs and approved by GTA.

The Offeror will also describe how it will design training experiences using standard principles of adult education and instructors' qualifications for developing and presenting training.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe any software tools it will use to administer these functions.

The Offeror will describe how it could collaborate with State training and education agencies to develop course content, and media production.

New Technology and Automation

GTA is interested in taking advantage of emerging technology developments that will:

- Enable a convergence of services across the Services where economies and increased user functionality can be accomplished.
- Leverage a combined infrastructure to obtain economies of scale for management, reduced cost, and Services integration.
- Enable the State to be more efficient and effective in providing higher levels of services to its citizens.

GTA envisions the Offeror performing the deployment of new technology and automation in support of the State's initiatives, systems optimization, systems improvement, strategic planning and policy goals. The goals of the State may include increasing the quality of government services, lowering the time for delivery of services, lowering the cost of providing services, providing additional avenues to accessing government services and information and increasing the flexibility of government.

The achievement of State goals and policy initiatives may require new technology in support of the achievement of business objectives. The Offeror must be responsive to needs and requirements of the State in accomplishing business objectives.

Functional Requirements

The Offeror's solution should support:

The GTA in the management and representation of technology products and service offerings to its clients.

The GTA to identify new products and Services to meet evolving State business requirements.

Providing technical expertise, assistance, and support for preparation of the long-range Information Systems plan and Equipment/Software Architecture plan, on a schedule specified by the GTA in support of the State's annual budget development cycle.

Providing the GTA with a detailed plan for transitioning the State to new technologies, including the removal and verification of billing adjustment processes for Services being terminated.

Participating, from time to time, in evaluations involving other service providers.

Cooperating with the GTA in researching and implementing automated tools that will improve the service and performance levels of the Services.

Participating with GTA on experimentation and research in leading edge Services solutions.

Working with GTA to conduct research in the innovative use of emerging Service technologies and provide advice and guidance to the GTA about potential benefits from new technologies.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will work with the State to support new technology and automation, including emerging and converging Services, methodologies, and techniques.

The Offeror will also describe how it will provide new technology services to include consulting, investigation, evaluation, acceptance, and recommendation of new technologies and automation of manual tasks.

Contact Center Support

GTA requires the Offeror to provide GTA with contact center support for use by the State in managing contacts from constituents. GTA defines a contact center as a convergence of technology subsystems (voice, video, e-mail and other data, both real time and non-real time) used to manage high volumes of inbound and outbound contacts.

A contact center typically includes call center capabilities that support multiple people/agents, a sophisticated Automatic Call Routing system, a computer for order/transaction entry and lookup on customer order/interaction. A contact center may also have a predictive dialer for handling a high number of outbound calls in a short amount of time.

Automatic call routing systems are computer-based systems that provide call routing for high-volume call transactions, with specialist answering "agent" stations and a sophisticated real-time call management system. The definition includes all call center-type systems that provide call handling capabilities and automatic call distribution, combined with a high degree of sophistication, in terms of dynamic call traffic management.

The contact center must be capable of deploying Customer Relationship Management (CRM) tools. GTA considers CRM to be a strategy with outcomes that optimize efficiency, minimize costs and increasing constituent satisfaction by organizing around constituent segments, fostering constituent-satisfying behaviors and implementing constituent-centric processes. CRM technologies should enable greater constituent insight, increased constituent access, more effective interactions, and integration throughout all constituent channels and back-office enterprise functions.

In order to support the States CRM objectives GTAe envisions the Offeror proposing the deployment of sophisticated call center features as the foundation upon which GTA can build an integrated CRM center. The contact center should be capable of:

- Integration with the State's information systems using standards based interfaces.
- Dispersed agent locations while providing transparent routing of calls and transparent agent groups via "virtual" call centers.
- Kiosk interaction where practical for constituents.
- Integration with e-gov systems that support electronic government interface with constituents.
- Video or voice contact with the contact center by constituents with just a click when browsing today's Internet or tomorrow's network accessible channel.

Functional Requirements

The Offeror solution should support:

Acting as single point of contact for all contact center integration related questions, problems and issues.

Providing daily operational, Install and MAC, programming, announcement production, and maintenance support of State contact centers.

Verification of operation and connectivity of contact center telephones and Workstation network adapters, and all other directly connected devices.

Assistance and support to GTA in specifying the appropriate configuration and install process for In-scope Equipment that will be attached to any contact center subsystem.

Providing voice recording for all inbound Automatic Call Distribution (ACD) calls and, optionally, for outbound calls

Provide predictive wait times for all inbound ACD calls.

Providing GTA with tools, access, and training required to validate all contact center systems performance

Meeting with GTA, on schedule agreed upon by GTA and Offeror, to review IVR performance, optimization levels, service history, problem resolution activities, and recommendations for improvement.

Performance of those activities required to continuously evaluate the principal performance indicators of contact center subsystem.

Proactively monitoring and managing contact center subsystems for congestion points and bottlenecks and make corrections.

Provision of an appropriate subsystem infrastructure to support future contact center subsystems, modern agent, supervisor, and systems applications.

Establishing and reporting on contact center trends.

Developing forecasts of contact center subsystem growth based on projected business and operational needs of the State.

Providing modern system administrative applications for configuration and administrative purposes via a secure web site that can be simultaneously accessed by multiple Designated Users.

Allowing Designated Users to access and make changes to contact center announcements as required, on a dial-up basis, through secured access.

Utilization of industry standards and best practice measures to protect the contact centers against unauthorized access and fraudulent use.

Assistance to State data applications programmers in developing required interfaces to support contact center subsystems.

Providing detailed analysis and management strategies for all contact center subsystems including:

Wiring and terminations from the system.

Power connections.

System testing, diagnostic and trouble shooting activities to verify proper operation.

On-going maintenance and support of the contact center.

Data network interfaces.

System and user features.

Voice network interfaces.

ACD queue specific configurations including call routing, queue timing and menus.

Allowing Designated Users to establish and manage call routing hierarchies, queue/hold parameters, recorded announcements, and other contact center features.

Automated attendant features including menus and prompts.

Voice recording and silent monitoring features.

Computer Telephony Integration (CTI), IVR, or ACD scripts or special programming.

Announcement-voice prompt recordings.

Coordination, procurement, and termination of all telecommunications trunks.

Agent/Supervisor and trainer headsets

Queue status display monitor wallboards.

Optional multi-source music/announcement on queue / music on hold service per site.

Standard and customized real-time, historical and forecasts reporting.

Agent/Supervisor and technical training.

Maintenance of inventories, location lists, and other documentation and information about the contact center subsystems and associated equipment.

Performing engineering and design for all existing contact center subsystems.

Providing integration coordination between all State contact centers and related databases, voice systems and network services.

Establishing access and reliability levels of service with Designated Users for each call center subsystem or service bureau solution.

Provision of a catalog description of available contact center and service bureau service options through a secure network channel.

Insuring all laws and licenses required for contact center technologies are met on the APA's behalf.

Management of the contact center subsystems Equipment and Software at all participating Sites.

Analyzing and proposing more cost effective contact center solutions and alternatives.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will describe its proposed contact center features and capabilities along with product literature, technical specifications, ease of use and forward-looking capabilities of replacement or new contact centers.

The Offeror will describe how it will support the State's contact center operations; provide Authorized User support, engineering design/support, and Services management.

The Offeror will describe previous experience in supporting call center Subsystems; including experience in designing, engineering, and integrating voice/data/video/fax/e-mail multimedia call centers.

The Offeror will submit examples of single Subsystem and multiple Subsystem call centers supported in environments similar to the State.

The Offeror will describe current strategies to support alternative communications capabilities such as Internet telephony, Internet chat applications, Internet "call me", integrated IVR systems, CTI and automated electronic mail distribution and management applications.

The Offeror will propose full service call center service bureau options, including an option for GTA or the State to staff a service bureau-provided call center with State employees rather than bureau personnel.

The Offeror will describe the life cycle of their system(s) and the upgrade requirements as well as how it intends to remain current following full implementation.

Installs and Moves, Adds, and Changes (Installs and MACs)

Installs and Moves, Adds and Changes consist of bundled work elements or service activities associated with a single request, resulting in enhancements or modifications to one or more of the In-scope Services. GTA envisions the Offeror including MAC's within Seat pricing.

The operational costs of the current State networks far exceed the capital cost of deployment. These operational costs have substantially limited the ability of the State to meet the needs of network users.

GTA envisions the Offeror deploying an infrastructure capable substantially minimizing the cost of MAC's by providing end users with the ability to make the majority of changes to the system. MACs could be minimized by enabling end-users with the ability to independently:

Change features on a phone, desktop, mobile terminal; possibly through a graphical user interface.

Relocating their phone or desktop; possibly by unplugging their phone from one jack and plugging into another.

Prewiring and preconnecting jacks to infrastructure ports.

Use of wireless technologies that enable end-user mobility.

Providing a secure network channel interface to an application that allows for the automated entry and status inquiry of MAC requests.

Functional Requirements

The Offeror's solution should support:

Provisioning of standard intervals for Service Installs and MACs.

Development and documentation in the Procedures Manual for procedures to handle requests for Services to include requests for shortened intervals (expedites), working the request outside of standard

business hours or on weekends, or changes made to the request after it has been submitted without changing the due date.

Install and MAC preparation activities that include:

Receiving Install and MAC orders from Designated Users and validate Install and MAC orders for correctness and proper authorization.

Provision of required components.

Conducting site surveys and coordinating physical space requirements.

Coordinating and making changes to the cabling infrastructure.

Tracking Install and MAC activity from initiation to completion.

Install and MAC execution to include:

Schedule and dispatch of appropriate technicians.

Configuration of the Equipment with the pre-defined State technology standards.

Installation and connection of Equipment to appropriate Services (e.g., LAN, telephones, etc.).

Coordination of all internal and external parties to execute the Install and MACs, minimizing impact to the business.

Installation of Software (including new Software and upgrades to existing Software), reloading data, and performing Equipment and Software configuration functions.

Install/connect of in-scope peripherals.

As requested by GTA, if installation occurs after hours, Offeror will also make available on-Site support the next working business day in order to resolve problems that occur as a result of the Install and MAC activities.

Verifying operation and connectivity of Workstation network adapters, and all other direct network-connected Equipment.

Testing Equipment, Software, and Services after Install and MAC to ensure appropriate functionality, and document Install and MAC results in accordance with the Procedures Manual.

Setting up appropriate access control for Services.

Provision of on-site support as required to resolve problems associated with large-scale implementations.

Provide for remote site Install and MACs.

Update the Offeror's Asset inventory management database upon completion of Install and MACs.

With respect to project Install and MACs:

Upon request, provide written proposals/quotes to Designated Users as required for Install and MACs after receipt of a valid order or site survey.

Schedule the procurement of circuits, installation of Equipment and installation of transport service, as well as the completion of all other activities necessary to achieve timely and successful project Install and MAC completion.

Securing and displaying all appropriate permits as required to complete any Install and MAC functions.

Fire-stopping all core drilled holes and firewall penetrations made in order to complete an Install and MAC.

Avoiding the disturbance of Site landscaping by using existing infrastructure (e.g., open conduit, existing cable plant) where feasible to support inter-building connections.

For any Install and MACs that touch or change State properties, returning the property to its original condition (e.g., landscaping, paint where building siding gets nicked, etc.).

For Service cancellations, make the necessary adjustments to the total number of Seats or relevant billable category. The cancellation should be recorded within and reflect the adjustment in the next billing cycle.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will perform Install and MAC functions for all Services. Install and MAC functions include but are not limited to: processes for obtaining approval from and communicating with the State, coordination of Sites and schedules, coordination with Equipment inside delivery and configuration, follow-up when problems occur, and updating the Asset management data base.

The Offeror will describe their standard intervals for Services and how they will deal with requests that are expedites, requirements for activity during non-standard work hours and/or cause changes in the scope of work where the scheduled date is desired to remain as originally scheduled.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

Offeror will describe its approach to incorporating Installs and MACs into Seat and/or Bundle configurations.

Asset Inventory Management

Asset inventory management includes the tools, processes and procedures used to manage a central database of Service Assets. This management will include but is not limited to the tracking, environmental planning, and return on investment analysis of all State and Offerors in-scope Assets.

GTA believes there are four classes of Assets in interest to the Offeror and the State. They are:

Those existing State Assets to be managed by the Offeror under this agreement.

Those assets, either existing or acquired in the future by the State or the Offeror on behalf of the State, installed or delivered by the Offeror.

Those assets which shall be the property of the Offeror, but identified and retained by the Asset Holding Company.

Those assets acquired by the Offeror to support the State but not included in the Asset Holding Company and which may be part of broader infrastructure and may be used by the Offeror to support customers, clients or parties other than the State.

GTA envisions the Offeror providing extensive and granular asset inventory management for those Assets described in Items 1, 2 and 3 above. The information is to be available to GTA on a real-time basis.

Functional Requirements

APAs will assist the Offeror in providing contact information (name, telephone, organization, and building location) for the users of individual Assets. APAs will also assist the Offeror in providing information about In-scope Assets.

The Offeror's solution should support:

Evaluation, provision, implementation and maintenance of tools and processes to track State technology Assets including Software license management (for only those Software program products addressed in Section 6.8).

Making the database accessible to Designated Users on a secure, network-accessible channel for querying and reporting.

Maintaining an Asset inventory management database for all Services, Equipment and Software provided and/or managed by Offeror and deployed at the Sites. Information maintained on all Services shall include:

Authorized User information

A complete profile of Authorized Users including Authorized User's account number(s), name (and address if different from billing address).

Account number.

Comments including miscellaneous notes, account history, etc.

Be updated by the Offeror within 24 hours of adds/moves/changes/deletions.

Technical Diagrams/drawings as requested.

Auditing the Asset inventory database on a quarterly basis, and provide audit results to GTA no later than the 10th business day following the last day of the previous quarter.

Providing Designated Users with read-only online access to the Asset inventory management database, produce periodic reports as necessary, and respond in a timely manner to queries and requests concerning the inventory data or supporting information.

Providing, upon request of GTA, a cumulative maintenance history on a specified piece of Equipment or specific Equipment makes and models.

Utilization of standards-based, automated Asset management tools for Equipment and Software that:

Support auto discovery and facilitate effective deployment and re-use of Offeror-owned technology Assets

Enable a common view in terms of information access and presentation by the State and Offeror.

Electronic links of such tools and processes to Offeror's call/problem management and Change Management tools and processes in order to enable the APAs to effectively utilize the information.

For each Service, the Offeror is to provide Asset management data in sufficient detail to enable APAs to manage other related business planning functions (e.g., applications systems deployment, refresh, billing, etc.).

When on-site service is required, that the Offeror's technician will verify the Asset inventory information related to the service call.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for its processes for maintaining and tracking an inventory of Assets, including Equipment and Software provided and/or managed by the Offeror and used solely in support of the State.

The Offeror will add to the inventory database Assets that are included as described above.

The Offeror will describe how the provisioning of these services will interrelate with the provisioning of other Services as identified in this RFP.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe any software tools or systems it will use to administer these functions and how GTA will access this tools/system.

Equipment Refresh

Equipment refresh is considered a standard activity in the service cycle of technology assets. Equipment refresh activities are focused toward ensuring the State's base of installed technology assets are appropriate for meeting the Service expectations of Authorized Users.

GTA envisions the Offeror refreshing equipment as required by changes within the States functional requirements. The changes may take place as the result of new functions required of the network, or as the result of the evolution of functions used on the network. Regardless of the objective of the change, the Offeror must refresh the network to accommodate the functional requirements of the State.

Functional Requirements

The Offeror's solution should support:

Performance of all operations required to support the refresh of in-scope Equipment. This will include: planning, associated change, problem and Asset management, de-installation, reinstallation, configuration, staging, and Authorized User orientation as otherwise specified.

Refreshing (procure and replace) In-scope Equipment with new In-scope Equipment as required to provide the Services and for the State to utilize current technology as directed by GTA. The refresh rate will be as agreed by GTA and the Offeror.

Financial responsibility for the Equipment to be procured and refreshed.

Performance of project management functions in the deployment of the Equipment refresh, including coordinating with GTA to determine project schedules.

The Offeror consulting with GTA and VPAs as required to identify emerging GTA and APA sponsored initiatives and determine impact as pertains to In-scope Equipment. If required, the Offeror, with approval of GTA, would develop and implement a plan to refresh necessary In-scope Equipment to support such emerging initiatives.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will provide a cost-effective approach to refresh all In-scope Equipment. Offeror will describe its technology refresh process and how it is responsive to changing business and market dynamics.

The Offeror will describe the life cycle of their system(s) and the upgrade requirements as well as how it intends to remain current following full implementation.

The Offeror will describe how it will identify opportunities to deploy new technology in the State and proactively bring proposals to GTA for review.

The Offeror will describe their strategy and assumptions used for Equipment refresh for each Service.

The Offeror will describe its experience and ability to ensure that APA's will receive the benefits of upgrades and advances in technology based on proposed platforms, architectures, etc. Include examples in delivering these functions within environments similar to the State.

Equipment Redeployment and Disposal

Equipment redeployment and disposal are considered to be standard activities in the life cycle management of Assets. These activities include making determinations regarding the appropriate disposition of Equipment (either redeployment or disposal), removal of Equipment to an appropriate location prior to disposal, purging all storage media to remove proprietary data, and updating the Asset inventory database.

Equipment will be disposed of when it is either: (i) technically and/or physically in an unusable condition, or (ii) no longer meets the APA's technical or performance requirements. Equipment that is technically and mechanically viable may, upon approval from GTA, be redeployed within the State.

It is a goal of the State to ensure the public health, promote resource conservation, and protect the environment. Ensuring the sustainability of the State's natural resources requires preventing waste and reducing the toxicity and hazardous constituents of discarded products. Disposal of electronic Equipment for wired and wireless telecommunications and information technology hardware make up one of the fastest growing segments of Georgia's waste stream. Most of these products contain RCRA-regulated hazardous materials that may require special handling. They also contain a substantial volume of potentially recyclable materials such as metals, plastics, and glass.

Functional Requirements

GTA reserves the right to require more stringent Equipment disposal methods as may be required by new State or federal regulations or when new and better disposal technologies become available.

The Offeror's solution should support:

Prior to redeployment or disposal, purging applicable storage media (either fixed or removable) to remove all traces of proprietary data. Information about data purging can be found at the following link: http://www.cerberussystems.com/INFOSEC/products/docusec3.htm.

Providing a recommendation to GTA as to the proposed disposition of the Equipment, either:

Store for redeployment.

Disposal.

Inclusion of shipping for Equipment to be moved or disposed of.

Entering all required information into the Offeror's Asset management database reflecting the disposition of the Equipment.

Disposal. The Offeror should:

Manage, in environmentally benign ways, with documentation, the final disposal of all Equipment purchased or leased by the Offeror during the Term.

Document final disposition. Documentation may include but is not limited to: open-market sales, return to manufacturer, or recycling to recover reusable or recyclable component parts or materials. The most appropriate disposal option will depend on the specific type of Equipment, its age, and functionality.

Not dispose of Equipment in a landfill in Georgia or any other state.

Return State-owned Equipment to the State's centrally located surplus and disposal facility.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for its process for redeploying and disposal of Equipment. In particular, the Offeror will describe its process for redeploying State-owned Equipment that is deemed viable by the Offeror for reuse.

The Offeror will also describe its process for meeting all federal, State, and local environmental regulations related to disposal of Equipment.

Descriptions should clearly describe how the Offeror will meet the functional requirements or provide an alternative solution(s).

Services Audits

Service Audits are periodic documented assessments of all Services with defined deliverables to include reports, Service environment recommendations and immediate

corrective action items required to stabilize any Services with findings that are out of tolerance.

The State must retain the right and responsibility, to perform periodic audits of the Services provided by the Offeror. The Offeror must provide the State with access to systems as required to perform the audit, participation in the audit as required, and participation in the support of resolution of deficiencies as identified by the audit process.

Functional Requirements

The Offeror's solution should support:

Cooperation with audits by the State's internal and/or external auditors.

Providing reports on audit findings.

Audit Services, at least one time each calendar year within 30 days of the Agreement anniversary date, making required adjustments, and reporting results to the State and to the billed Authorized Users.

LAN/WAN Security audits and reports. The Offeror should:

Perform audits of the LAN/WAN as required and report findings to the State.

Provide written responses to both internal and external technology audits.

Provide change recommendations that will be incorporated into internal technology health checks, as approved by GTA.

Provide audits on the number of Seats and other recurring billing categories and reconcile with Offeror bills.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will perform audits of the Services, including details about which Services will be audited, the frequency of the audits, and templates of reports that will be provided to GTA regarding audit findings.

Wiring and Physical Cable Plant Maintenance and Installation

Wiring and Physical Cable Plant maintenance and installation services will be done in accordance with the State's established codes, standards and practices, and include:

- Repair and upkeep of existing embedded inside and outside plant infrastructure cabling including pathways, building riser cabling, and horizontal distribution media.

- Installation of new or additional inside and outside plant infrastructure cabling including pathways, building riser cabling and horizontal distribution media with pathways.

GTA envisions the Offeror taking responsibility to provide APAs with wiring as required to meet the functional requirements of the State. This may result in the need for the Offeror to provide new and/or replacement wiring. Installation of the new and/or replacement wiring will be performed by the Offeror at no additional cost.

Functional Requirements

The Offeror's solution should support:

Responsibility for correction of all problems resulting from malfunctions in the Physical Cable Plant.

Performing the design, installation, and termination of all infrastructure cable plant necessary to meet APA's requirements for In-scope Services.

Supplying cabling that is neatly laced, as applicable, dressed, sheathed and adequately supported in accordance with Building Industry Consulting Service International (BICSI) guidelines and the State's published infrastructure cabling specifications.

Providing cable supports when required outside the room in which Equipment is located. Offeror agrees to provide cables with a flame resistant sheath for horizontal inside cabling requirements.

That all cabling provided by the Offeror shall adhere to State published cabling specifications and BICSI guidelines, identified in the State Technical Paper for Infrastructure. (Appendix E)

For all cabling outside the room in which Equipment is located shall be connected in conduits, raceways or runways.

Creation and maintenance of cable plant records for all State infrastructure cabling locations.

Providing GTA with updated cable plant records via secure, network-accessible channel to include all relevant cable record documentation.

Under certain conditions, providing repair services to State-owned infrastructure cabling (e.g., fiber, horizontal voice and data distribution, outside plant, coax etc.) that are not maintained by the Offeror under the terms and conditions of the Agreement such as GDOT fiber. These repairs will be invoiced to the State on a "time and materials basis" per occurrence as requested by the State.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will install and maintain the Physical Cable Plant.

The Offeror will describe how it will install, maintain and repair the Physical Cable Plant associated with all in-scope Services, including the implementation and updating of a cable records management system.

It is our desire that the Offeror use components having standards-based interfaces that will facilitate the highest level of interoperability on all infrastructure cabling.

Site Survey and Physical Environment

Site survey Services include all activities and events related to projects that involve changes to the physical environment of existing Sites or implementation of new sites that APAs may require during the Term. The parties involved may include, but are not limited to architects, building contractors, and State personnel.

These activities are performed to determine specific installation requirements related to the physical environment for implementation of Services or changes to existing Services.

These activities include documentation of design criteria, requirements for resources, and physical environment considerations.

Functional Requirements

[Modified per Addendum no. 3] Subject to the agreement, GTA may request Site surveys on a project by project basis to support activities.

The Offeror's solution should support:

For new or existing State Sites, managing the physical survey of each site to determine site features implementation readiness, and specific installation requirements for all requested Services.

For new or existing Sites, assistance to the architect in design of the system and working with the general contractor as the installer.

Performing Site visits with the oversight of Designated Users.

Site survey information being documented to include the:

Complete scope of work for requested project requirements (e.g., power/UPS, space, grounding requirements, Equipment and Software, other relevant environmental)

Complete materials list for scope of work.

Facility utilization plan.

Coordination of all on-Site activities with appropriate Site property management personnel, and following of all facility rules related to alterations to the physical plant prior to beginning any job.

Providing documentation of work that alters a Site physical plan to Designated Users and property management personnel.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror shall provide an overview for how it will manage the maintenance and updating of Site information for existing Sites and, subject to the Change Management Procedures, as necessary for new sites.

The Offeror will describe and provide examples of what site documentation will be provided to present results of site surveys.

The Offeror will describe its experience in developing sites for projects of size and scope found in environments similar to the State.

Lab Testing

Lab testing Services include testing and results documentation of any new product or Service prior to introduction into the APA's production environment.

The capabilities of the Services offered by the Offeror are integral with achieving the policy objectives of the State. As such, it is imperative that APAs be aware of the capabilities and limitations of technologies and Services provided by the Offeror. The GTA envisions the Offeror involving APAs in the development and release of services by providing the State with insight into the testing and performance results of new services.

Furthermore, the State's public education institutions would benefit from access to services that promote educational research activities. GTA envisions the Offeror offering services for use in educational research.

Functional Requirements

The Offeror's solution should support:

Provision of laboratory environments that simulate the State's production environment.

Submitting to the GTA a test plan for all new Equipment and Software.

Providing a comprehensive and rigorous testing process, systems integration testing, connectivity testing, load testing and application interconnectivity testing on all new versions of Equipment and Software.

Providing access to test environments to APAs when appropriate and under mutually agreed upon conditions.

Making available the Offeror's integration labs and performing integration testing in conjunction with GTA.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will provide thorough testing of new versions of Equipment and Software prior to deployment. This includes the construction and maintenance of laboratory systems that simulate the State's production environment. Offeror will provide results of testing upon request.

Describe the participatory role the State could expect to play within the testing of network services.

Describe the opportunities for research available to the State.

Operations Documentation

Operations documentation includes the continuing development, management and retention of process and procedures records that outline the Offeror's day-to-day business practices as they relate to the Services. This includes the Procedures Manual to be developed by the Offeror and approved by GTA.

Operations documentation includes the recording of information pertinent or critical to the operation of the Services. This information can be in written text, lists, databases, graphics, maps, VRML, etc.

Functional Requirements

The Offeror's solution should support:

Creation and maintenance of documentation in a hierarchical structure suitable for publication on-line to Designated Users.

Providing as-built drawings, connectivity maps and/or tables which describe the physical and logical structure of the networks or systems installed. Maintaining current documentation in hard and soft copy on all operations procedures, Services, Equipment and Software for which Offeror is responsible to include:

Operations procedures and Services.

Application procedures that affect operations.

Authorized User procedures that affect operations.

Documentation audits and action as follows:

Regular audits of documentation for completeness and accuracy in order to verify that all documentation is present, organized, readable, and updated.

Correction of such documentation where it is determined that documentation is inaccurate (e.g., erroneous or out of date).

Ensuring that the provision of all Services is consistent with current documentation.

Ensuring that all documentation maintained by Offeror is be subject to approval by the State and will conform to documentation standards agreed upon between the Parties.

Helping the State confirm its business requirements.

Identifying information and associated technology needs.

Helping identify projects to be performed, defining schedules, and preparing cost benefit analyses.

Helping to specify the Equipment/Software Architecture and participating in continuously keeping the State's Information Technology Architecture current.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for the manner in which documentation will be created and maintained for the Services. In this description, the Offeror will include the structure for the documentation and tools that will be used.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe any software tools it will use to assist with the development of documentation.

The Offeror will include the number of documentation copies it will provide to the State and the Site in its descriptions.

Descriptions should clearly describe how the Offeror will meet the functional requirements or provide an alternative solution(s).

Regulations

Regulations includes those laws, rules, procedures and/or processes relating to the Services and defined by a recognized local, State, federal or international governing body that must be followed whenever applicable.

Functional Requirements

The Offeror's solution should support:

Compliance with all current and emerging regulations for each affected Services area, including but not limited to those of the:

Federal Communications Commission (FCC).

Georgia Public Service Commission (GPSC).

Federal, State, and local rules, regulations, and laws governing the Services.

Americans with Disabilities Act (ADA).

Silent service monitoring and recording.

911/E911 services.

Compliance with RF licensing regulations, including the filing, and keeping current, of any necessary licenses.

CJIS 2000, and HIPAA.

Identifying, evaluating and recommending modifications to the Services environment as required to maintain compliance with local, regional and international regulatory changes applicable to Services.

Performing such modifications within timeframes agreed to by the State.

That where Service or product providers must make modifications to their services or technology platforms to achieve compliance, Offeror will, upon GTA's request, oversee these activities and verify that they are performed within acceptable timeframes.

Providing progress reports to GTA at regular intervals.

Keeping abreast of and advising GTA about emerging governmental regulations.

For State systems that interconnect with mandated federal systems, the Offeror will follow ISO/IEC 15408 Common Criteria guidelines necessary to comply with Federal Requirements or as the State requests.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will perform Services in such a manner that they comply with current local, State, federal, and international regulations, and explicitly address Items 1.a through 1.h listed above. Include the approach to remain continuously current with regulatory changes.

Quality Assurance and Continuous Improvement

The quality and continuous improvement of Services is of great interest to the State.

For the most part, the State's measurement and comparison processes are intermittent, manual and project- and function-based. GTA envisions the Offeror providing methods and procedures that serve to continue to transform Services. GTA desires to move to a more continuous, decision-based, integrated set of processes for measurement and comparison. GTA would like these processes to form the basis of a consistent continuous-improvement program.

Functional Requirements

The Offeror's solution should support:

Writing and maintaining procedures on all quality assurance activities and document them in the Procedures Manual.

Writing and maintaining procedures on all continuous improvement activities and document them in the Procedures Manual.

Creating a quality assurance manual and ensure compliance.

Maintenance of Equipment and Software quality consistent with industry practices.

Cooperation with GTA's quality assurance audits.

Documenting and implementing process improvement.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will define its philosophy of quality; not only what it is, but also how it is measured and maintained, and how its measurements compare to industry benchmarks for like Services.

Describe the Offeror's certifications and commitments to quality assurance and continuous improvement.

The Offeror will describe if they are committed to using industry standard technology quality assurance and continuous improvement

processes, e.g. ISO 9000/9001/9002, CMM, and ITIL. If so, which ones?

The Offeror will describe its quality assurance and continuous improvement programs and how its tools and processes will be utilized to provide GTA a quality solution that is at a level consistent with acceptable industry practices and the State's current standards.

The Offeror will describe its commitment to bench marking and measurement of performance; its commitment to a comparison of current performance with benchmarks and strategic objectives; its commitment to establishing strategies for improvement in cooperation with GTA; and the use of best practices for establishing improvement action plans.

Descriptions should clearly describe how the Offeror will meet the functional requirements or provide an alternative solution(s).

Customer Satisfaction Surveys

Customer Satisfaction is a primary method the State will use to determine the success of the Offeror and GTA. It is imperative that the Offeror be capable of responding to needs and requirements found as a result of the surveys.

Customer satisfaction surveys include the creation of survey instruments and a random selection of Authorized Users to objectively document and measure their satisfaction with the Services. GTA will retain the right to develop and/or approve the content of all survey instruments prior to their distribution.

GTA envisions the Offeror performing an annual Customer Satisfaction Survey collaboratively with GTA. The Offeror will distribute and tabulate the surveys. The results will be presented to GTA for review.

Functional Requirements

The Offeror's solution should support:

Surveying the following classes of Authorized Users:

The GTA Executive Director to be surveyed on a monthly basis.

VIP users, to include select members of the Governor's senior staff, select members of BOR senior staff, state agency commissioners, state authority executive directors, university system presidents and senior administrative officers of participating Political Subdivisions to be surveyed quarterly

Designated Users, state agency IT directors and university CIO's to be surveyed quarterly.

All Authorized Users to be surveyed continuously online with results cleared and tabulated each calendar month.

Collaboration with the GTA on the creation of the instrument used for conducting the survey.

Conducting surveys and reporting the results to the GTA.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will work with the State to measure Service Levels as requested, provide data on performance and collaboratively identify how Service improvements can be made.

Project Management

Project management includes disciplines related to implementation of Equipment, Software, or Services. These projects may include changes to existing or implementation of new Services, Software, or Equipment.

These disciplines include defining the project scope, its goals and objectives, timelines, milestones, communications strategies, and coordination of project deliverables with Designated and Authorized Users.

The GTA envisions the Offeror establishing a Project Management Office for the duration of the contract. Due to the critical importance of the PMO activities, the GTA envisions the Offeror providing highly qualified individuals within the PMO.

Functional Requirements

The Offeror's solution should support:

Implementation of a project management methodology including the use of project management tools approved by GTA.

Preparing proposals in response to State requests for technical solutions and pricing.

Development of functional and technical requirements and project plans to include cost, ongoing maintenance support requirements, risk, alternatives, recommendations, with specific references to any variances to GTA standards.

Management of all Offeror tasks across Service families, coordinating with appropriate GTA personnel and other service and product providers.

Presentation of up to date status reports, and identification of potential bottlenecks and problems to GTA as requested.

Meeting with representatives of GTA as necessary and appropriate to manage and deliver the Services' projects effectively.

Participation in and cooperation with the various account management committees called for by the Agreement and the procedures adopted by the Parties to charter each such committee.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will perform project management and how it will ensure these processes are followed for Services projects.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe any software tools it will use to administer these functions.

On-Going Reviews

On-going reviews include those activities related to:

- Planned and regular communications between the Parties.
- Oversight by GTA of Offeror Services delivery, management, and operations.
- Coordination of Services delivery and management between APAs.
- Planning for projects, new Services strategies, and consideration of how emerging technologies will meet the State's current and emerging business requirements.

The Offeror and the GTA Telecommunications Division or its designee will meet on a regularly scheduled basis with the schedule to be agreed to between the Parties.

Functional Requirements

The Offeror's solution should support:

Service reviews conducted weekly, (or on a schedule mutually agreed to between the Parties), with GTA to include:

Activity schedules.

Operational readiness to perform project activities.

Discussion of operational problems and issues that may impact project deliverables.

Adjustment of schedules and resources as required to meet State objectives.

Identification of any future plans or anticipated future problems.

Monthly operational reviews of the Service Levels including the following Service reviews:

Service outage incidents.

Performance and availability reports. Provide "Get Well Plan" for all items not meeting threshold service level requirements.

Service utilization, capacity information, and availability.

Root cause analyses and remedial actions undertaken for Service outages.

Quarterly capacity planning reviews to:

Review Service utilization and related capacity management plans.

Review ongoing and future business plans, issues, and requirements (and their impact on utilization).

Formulate recommendations for State.

Discuss technologies applicable to such issues and requirements and formulate recommendations for State.

Providing the State with the capability to monitor compliance with performance standards, including access to databases used by Offeror in management of the Services.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will provide communications to the GTA Telecommunications Division or its designee regarding management and operations of the Services and status of on-going projects.

The Offeror will describe its experience in providing and conducting progress reviews in environments similar to the State.

Reporting

Reporting includes analytical, statistical and performance measurement reports and documentation required by the GTA to support Agreement compliance.

Reporting will allow the State to forecast and prepare for necessary upgrades and changes to the enterprise environment to meet changing business or technical requirements.

Functional Requirements

The GTA will determine which Designated Users will have access to the reports.

The Offeror's solution should support:

Providing Designated Users with the capability to generate ad-hoc and custom reports by making Services information and databases (e.g., Asset inventory) available on a secure, network-accessible channel with appropriate security preventing unauthorized access.

Providing report data in web-browseable hierarchical HTML and downloadable to the APA's personal productivity tools (e.g. Microsoft Office).

All reports to be provided at the agency/location level or by measured system (e.g., IVRs), except as otherwise expressly defined within this SOW.

Making standard monthly reports available on a date to be determined by GTA except as defined elsewhere in this Statement of Work.

Designated Users having electronic access using standard query tools to all information and databases related to Services.

Consolidation of all monthly reports into an annual summary by anniversary date of the agreement, and annual summaries will be retained for the Term of the Agreement.

Reports required for all Services monthly by Site, agency and billing account number. At a minimum, such reports will include:

Order Fulfillment:

All Services, described at the lowest detailed level, all Services installed, moved, and disconnected during the previous month.

Charges.

Summary reports showing average installation, move, and disconnect times.

Order fulfillment reports showing all instances where the allowed times were exceeded to show date of order, due date based on allowed interval, actual date order completed, and reason for delays.

Problem reports:

Implement a process for tracking and reporting Help Desk and other problem activity by APAs, including, at a minimum the Offeror's standard Help Desk reports showing type of problem, cause, restoration actions and times, and applicable charges.

On a monthly basis and by MPA, analyze call trends, perform root-cause analysis, and recommend actions to reduce calls.

If restoration times exceed those allowed, report will also include reason for delay.

Reports as detailed in the Agreement and as deemed necessary from time to time by GTA.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will offer a reporting solution that will assist GTA in the management of the Services. GTA seeks innovative solutions to the management of the reporting requirements necessitated by such a large-scale & multi-service procurement.

The Offeror should describe how it will aggregate reporting across functional service areas while also making sufficient detail available as

necessary. The Offeror will provide hard copies of reports as requested by GTA.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe any software tools it will use to administer these functions and how the output can transfer into the State's standard personal productivity tools (e.g. Microsoft Office).

The Offeror will provide a sample list with examples of what reports are intended to be provided to GTA.

The Offeror will describe to what degree GTA will be able to independently run ad hoc reports.

Décor & Historic Preservation

There are many locations throughout the State of Georgia that have customized decorating and design (e.g., Capitol Building custom booths, antique phone desktop Equipment, campus landscaping, etc.). Some are historic sites. The State wishes to preserve the integrity of all such Sites.

Functional Requirements

The Offeror's solution should support:

Preservation of and respect for established building decor and the integrity of historic sites while performing any and all communications Services work.

Provide the State with detailed schematics of all historic preservation adaptations and customized Equipment solutions as they are identified during the course of routine maintenance activities.

Conform with all published laws, codes, rules and regulations related to performing work in historic structures.

Offer's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will confirm its commitment to preserving these historic entities, landscape designs and building decor.

Offeror Personnel Qualifications

The Offeror personnel assigned to perform the Services will be fully qualified, professionally certified where appropriate, and committed to perform the Services. In addition, all Offeror personnel will have backgrounds satisfactory to the individual APA's receiving Services. For the purposes of this section "Offeror's Personnel" are those employees assigned to perform Services required under this RFP.

Functional Requirements

GTA retains the right to require the Offeror to remove any personnel that the State feels do not meet its Service or personnel requirements.

APAs will provide name badges for Offeror personnel that identify them as Contractors of the State.

The Offeror's personnel will:

Have a social security card if a United States citizen.

Have a green card if not a United States citizen.

Be able to communicate in English.

Pass background checks as required by the individual State entities where Offeror personnel are engaged.

If requested by an APA entity receiving Services, Offeror personnel will not begin work until criminal and/or driving background investigations have been completed by the Offeror, and the results have been

approved by the APA receiving Services. Background Investigations will:

Be documented in writing from a security investigation provider approved by the State.

Examine at a minimum the last seven (7) years of an individual's history for any criminal activity and the last three (3) years for any driving violations.

For Offeror personnel who have not been residents of the State of Georgia for a year or more, background investigations will be conducted in the originating state or country.

Observe APA's workplace, health, safety, sanitation and personal conduct guidelines and directions.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

Third Party Relationships

The State currently utilizes the services of a number of third-party contractors to supplement its personnel performing tasks within the scope of the Services described in this RFP. The State's intent is to significantly reduce, or eliminate, the number of such third-party relationships. The State's current third-party agreements relating to Services described in this RFP will be:

- Canceled;
- Assigned and assumed by the selected Offeror or
- If not cancelable or assignable, then managed by the selected Offeror as the State's representative or agent.

In support of those third party contracts that are not assigned, but are managed by the Offeror (i.e. Managed Third Parties or MTPs), the State shall:

- Consider in good faith, the selection, modification or termination recommendations of Offeror with respect to the performance and cost benefit of existing and future MTPs.
- Provide reasonable assistance to Offeror in the MTP escalation process.
- Provide Offeror a letter of agency for each MTP where necessary.

Third Party contract information is contained in Appendix I. Note, third party agreements involving the lease of unencumbered real property;

rights of way; or access rights are not included within the scope of this RFP.

Assigned Third Party Functional Requirements

The Offeror's solution should:

The Offeror will be responsible for obtaining consents from all third parties in connection with assignments and assumptions of the State's agreements, unless previously obtained by the State.

Confirm that the Offeror will be legally, including financially, responsible for all of the State's obligations, terms and conditions contained within third party contracts assigned to and assumed by the Offeror.

Managed Third Party Functional Requirements

The Offeror's solution should:

Manage the MTPs, including monitoring operational day-to-day service delivery, monitoring performance, escalating problems for resolution, and maintaining technical support relationships.

Treat the invoiced charges of Managed Third Parties as Offeror's Expenses, paying such invoices directly or reimbursing the State where such direct payment is not possible.

Be responsible for meeting or exceeding the applicable Service Levels even where doing so is dependent on the provision of Services by a MTP.

As requested, work with GTA to manage new and existing contractual relationships between GTA and MTPs as needed to provide the Services.

Assume financial liability for, and indemnify the State against any related fines or fees that may be due from the State due to the acts or omissions of a MTP.

Oversee MTP delivery of Services and compliance with the Service Levels and the performance standards contained in State's agreement with the MTP.

Notify State and the MTP of each MTP failure to perform in accordance with the Service Levels or the performance standards or other terms and conditions contained in State's agreement with the MTP.

Escalate MTP performance failures to MTP management as necessary to achieve timely resolution.

Monitor and manage the MTP's efforts to remedy a failure.

Communicate to the State the status of the MTP's efforts to remedy a failure.

Recommend retention, replacement, modification, or termination of all MTPs.

Assure that all record keeping requirements are observed with respect to an MTP. The Offeror will be ultimately accountable for any financial or

operational records and the sufficiency of information in support of audits that the State may wish to engage in from time to time.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

Given that a significant amount of institutional knowledge resides with third-party contractors, describe the role, if any, they will play in your organization's proposed solution. Describe your organization's approach to any necessary transition of functions from or to these contractors, including assignment and assumption of existing contracts, subcontracting, or cancellation of contracts.

Is your organization willing to manage and assume financial, administrative, and legal responsibility for the State's current third-party telecommunications-related agreements, including associated transfer costs, if any? Explain.

To the extent that the State continues to maintain relationships with other providers of telecommunications services during the term of the relationship with your organization, is your organization willing to act as the State's prime contractor with respect to such third parties? If not, explain. Describe your organization's approach to any necessary transition of functions from or to these providers, including assignment and assumption of existing contracts, subcontracting, or cancellation of contracts.

The Offeror shall assure that none of the Services or other items provided to the State by Offeror shall be adversely affected by, or shall adversely affect those of any other of the State's third-party contractors, whether as to functionality, speed, Service Levels, interconnectivity, reliability, availability, performance, response times, or otherwise. Will your organization provide these assurances to GTA? Explain.

Distributed Computing General

Distributed Computing includes the management, operations support, procurement, and deployment for Local Area Networks (LANs), including Equipment and Software, within In-scope Sites, as well as the provisioning and management of Workstation (Desktop and Laptop).

As of the Effective Date, Offeror will assume responsibility for the operation, management and support of the Distributed Computing environment.

Initiatives to be addressed in the Offeror's plan for this environment will include: (i) improved processes and automation, (ii) standardized configuration of the Equipment and Software, (iii) automated Equipment and Software support, and (iv) improved service.

Current Environment

Local Area Network (LAN) support, by current definition, is considered to the LAN typically begins at the LAN interface of the router (router, ATM edge device, or layer 3 switch and includes support of the hubs, switches, servers) to the desktop. In most instances, State entities are responsible for planning, implementing, and supporting their own LANs. (GTA IT provides services for a few State agencies too small in size to warrant a support staff. These consulting services are provided by LAN engineers and include design, installation and maintenance and special projects as needed. Generally, the agency has a contact individual on staff that also resolves simple problems. Other small entities may contract with outside vendors for LAN services.)

There are no statewide standards for equipment or network software. The most common network operating systems in use are Novell, Microsoft and UNIX, varying greatly in version from very dated to most current.

LAN services offered vary greatly across the State. In many installations, it is extremely difficult to separate the LAN and desktop elements since the desktop is dependent on the LAN for many services such as electronic software distribution, virus protection, e-mail, back ups, file, print and database services, etc. Many State entities also have Intranet, application, inventory, firewall services, and remote dial in solutions.

Desktop-Like LANs, desktops in the State vary widely in make and model, operating system, software in use, and network connectivity. Standards, if they exist at all, vary from entity to entity. PCs, MACs, NCTs, and 3270 terminals are used by various entities as desktop devices. Printing may be accomplished in a variety of ways, e.g. through locally attached printers, networked printers or by various mainframe initiated printing processes. Equipment is often purchased using GTA contracts created for statewide use. GTA is not confident that the attached survey is the complete inventory of statewide equipment or software.

Many devices need to access the State's GO Network to use mainframe applications. Some attach using the Channel Interface Processor (CIP) interface over IP, but many connect through SNA, using controllers and SAA gateways.

Desktop software varies widely from user to user even within the same entity due to both varying business needs and a lack of standards. Many entities' desktops are connected to a Local Area Network (LAN), which connects to the Wide Area Network (WAN). This facilitates access to GTA provided services such as inter-agency email, Internet access, file transfer, etc. Desktop operating systems vary statewide as well. Desktop technological expertise as well as methods and quality of support vary from entity to entity. Many agencies use the GTA contract for PC hardware maintenance that provides for repair or replacement of a wide variety of equipment. The GTA External IT Help Desk dispatches the vendor statewide. The GTA Installation, Maintenance and Support (IM&S) group provides field service statewide for network problems including individual workstation connectivity issues.

The GTA Internal Network Support (INS) group can be used as an example of an entity's approach to desktop Services. GTA supports approximately 1400 end users in 21 Sites statewide. Users' responsibilities range from basic administrative duties to in-depth software development activities. INS provides a wide range of support services including desktop provisioning, problem tracking and resolution as well as LAN administration, design and configuration. IM&S staff assists the INS group with desktop support at the District Offices.

Installation and MAC requests (approximately 500 per month) are also handled by the Desktop Support staff and handed off appropriately when the purchase of hardware or software is required. Directory services-based electronic software distribution (ESD) techniques are employed to deliver virtually all 200+ software packages in GTA.

All incoming and outgoing Internet e-mail is scanned for viruses. Most viruses are discovered before they reach the desktop by server-based virus scanners, but desktop scanning is done to eliminate virus threats from floppy disks, etc. Remote access to the GTA systems is available to remote users via dial-up and the Internet. Inappropriate World Wide Web content is filtered and Internet usage reports are available to management for review.

There are multiple e-mail systems running throughout the State (GroupWise, Outlook, Lotus Notes, etc.). They are operating on hundreds of Servers statewide.

Desired State

The GTA desires to adopt a statewide standard for equipment and LAN components such that the disparities between users with regard to functionality, interoperability and support are reduced. The GTA also wishes to reduce the risk of business interruption to the APAs through more consistent management of these assets.

APA personnel should be able to expect uniform access to software (as applicable to their job function) and a highly reliable, consistent level of service with respect to Services such as repairs & maintenance, backup & recovery, and Help Desk support.

GTA also desires implementation of an enterprise-wide system management methodology that enables remote monitoring and diagnostics of all network devices resulting in improved Service Levels.

It is our desire that the Offeror use components utilizing standards-based interfaces that will facilitate the highest level of interoperability on all network components.

The GTA also desires to use LAN standards that allow for the maximum possible amount of convergence within a facility. The GTA believes convergence within the LAN will enable the greatest amount of flexibility in the deployment of voice, video and data applications.

The Offeror will become responsible for the deployment and maintenance of the State's facility wiring infrastructure.

The State would like to take advantage of the economies that may be achieved through the use of convergence within the desktop and LAN. This would include the consolidation of hardware and software platforms where possible, centralized facilities where appropriate, and consolidation of single wiring infrastructure where possible.

Workstation Support

Workstation support includes support services, including problem diagnosis and resolution for Workstation Equipment and Software for Authorized Users. Resolution may be provided remotely or on-Site. (Equipment break/fix is a separate Service category.)

Functional Requirements

Authorized Users with Workstations attached to the LAN will use LAN Servers for storage of data.

The Offeror's solution should support:

Providing support services for Authorized Users in central and remote Sites, including Authorized Users who are traveling, remotely accessing LAN-based services, or located at a non-connected site.

Providing on-Site field service to Sites as required.

Provision of secure access for remotely connected mobile workers to network services.

The Offeror must provide installed on each new Workstation or Server the following minimum configuration at the time of installation. Furthermore, the Offeror needs to maintain, at a minimum, the following Software items at current operating releases as defined elsewhere in this SOW.

The State's Standard Operating System. (The current standard is Microsoft Windows XP.)

The State's personal productivity suite Software according to the GTA standard. (The current standard is Microsoft Office XP Professional)

Virus protection Software according to the GTA standard.

Connection to State's WAN.

Electronic mail.

Browser

Utility packages such as screen capture, file compression, graphics viewers, PDA sync software, Acrobat, etc.

Capability to access mainframe and/or application Servers.

Access to LAN and Server applications, including file and print services.

Internet/Intranet connectivity.

Providing Authorized User support and problem resolution for any additional software installed at the request of Designated Users on Workstations and Servers.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will provide support, advice and assistance to GTA in order to meet the needs for Workstation Support of Authorized Users.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

Electronic Mail Support

Electronic mail (e-mail) support includes support for electronic mail services including connectivity with Internet mail services. This includes support for the e-mail applications, the In-scope e-mail Servers, and e-mail Authorized User account management. The Offeror must ensure that every Authorized User has e-mail and calendaring capabilities with statewide seamless operational capability.

Functional Requirements

The Offeror's solution should support:

Responsibility for deploying and supporting GTA approved e-mail application environment within the State.

Managing the MPA's standard e-mail Servers, except as otherwise defined in Section 6.7.8.

Administration and maintenance of electronic mail services, including e-mail application software, Servers, and related infrastructure.

Unified messaging.

E-mail security as needed that:

Provides a secure ("writer to reader") e-mail application system to Authorized Users requiring additional security for their e-mail.

Provides enhanced authentication measures and the capability to digitally sign and encrypt/decrypt messages and attachments.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

For all Authorized Users, the Offeror will provide an overview for its strategy for the support of electronic mail to include: mail, directory service, database management, remote Authorized User access and electronic mail applications services.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe its strategy to provide unified messaging Service.

The Offeror will describe their approach for providing e-mail access to Authorized Users.

Virus Prevention and Protection Services

The Offeror will be responsible for virus prevention and protection services including the operation, maintenance, and administration of the Offeror's virus protection solution (including Equipment and Software), and response to Virus attacks and incidents.

The Offeror will establish, deploy and manage an enterprise-wide virus management program for all State LANs, In-scope servers, and network attached Workstations. Including virus management systems to automatically scan, perform system and component isolation, and initiative virus protection software at Vendor's current release levels in accordance with Service Level objectives. The Offeror will be responsible for implementing a virus awareness-training program and will immediately notify GTA upon detection of any virus.

These services also include proactive identification of Virus threats from within and without the State, monitoring of State systems in order to prevent the spread of Viruses on State Equipment and Software, and notification to Designated Users about the actual or potential threat of Viruses to APAs.

Functional Requirements

The Offeror must secure the approval of the GTA for the Virus protection solution Equipment and Software selected by the Offeror.

The Offeror's solution should support:

Selection, installation and configuration of a Virus protection solution, including Equipment and Software, of sufficient effectiveness to protect all Equipment and Software capable of being infected with Viruses.

The capability to scan diskettes or hard drives upon demand.

Testing, installing, updating, operating and maintaining the Virus protection solution on all Equipment capable of being infected by Viruses.

Virus scans on all incoming and outgoing e-mail.

Virus scans on all files being transferred to and from the Equipment capable of being infected by Viruses.

Updates to Virus Equipment and Software, including any necessary Virus definitions, on a regular and ongoing basis in accordance with the timeframes set in the Service Levels and Procedures Manual.

Upon detection of a Virus, the Offeror should:

Take immediate steps to notify the Help Desk, assess the scope of damage, and arrest the spread of and progressive damage from the Virus, and eradicate the Virus.

Initiate such actions necessary to salvage or restore as much of the impacted file Server data and Software as possible.

Restore the impacted Equipment capable of being affected by Viruses to the standard configuration.

Conferring with GTA on the selection of the Virus protection Software.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will describe its strategy for implementing a State-wide virus management program, including automation, controls, and tools needed to implement and provide centralized monitoring, automated alerts, and virus removal upon detection.

The Offeror will provide an overview for how it will respond to Virus incidents, proactively provide Virus protection for all Equipment and Software capable of being infected with Viruses, and ensure the Virus protection Equipment and Software and Virus definitions are updated.

Describe you approach for providing immediate notification to GTA upon virus detection and your process for on-going communication regarding status of detected viruses.

Describe how you expect GTA to be involved in the virus management program.

Equipment and Software Configurations

Equipment and Software configuration Services include the design, documentation, and maintenance of Workstation Equipment and Software configurations.

Functional Requirements

The Offeror's solution should support:

Proposing hardware standards to GTA for approval.

Proposing Equipment and Software configurations for Workstations and Servers to GTA for GTA's approval. Configurations may be modified and amended as approved or requested by GTA, and in agreement with the Offeror which shall not be unreasonably withheld. There may be multiple configurations in effect at the same time.

Documentation, implementation and maintenance of the GTA-approved configurations throughout the supported environment.

Performing analyses of the Equipment and Software environment in order to (i) identify areas of non-compliance, (ii) evaluate new and emerging technologies and (iii) select technologies that will support the changing business requirements of the State.

Proposing how the Offeror will handle exceptional configurations when required to meet unique requirements of APA's.

Software testing:

Where Software, upgrades or patches affect or could affect custom code, the Offeror will assist in unit testing with APA applications personnel and in Authorized User acceptance testing with the applications personnel and affected Authorized User base.

Coordination of testing and distribution with applications personnel and Designated Users as appropriate.

Maintaining multiple master copies of all Software for which the Offeror has distribution responsibility. These copies are to be stored in a controlled environment suitable for the long term storage of magnetic media.

Provide centrally managed backup capability for select individual workstations.

Provide all Authorized Users with access to all software and hardware manufacturer user documentation.

Maintain current versions of system utilities and other software. Coordinate maintenance and release upgrades in accordance with State Service Levels.

Replacing fixed function terminals, 3270-type, SNA-connected Workstations, modem sharing devices, SAA Gateways and SNA-type printer devices (to include 5080 class Equipment), which connect to 32xx controllers or other SNA control units with Workstations and terminal emulation capabilities as required.

At a minimum, Workstation hardware configuration that meets the median configuration recommendation provided by the vendor for the n-1 version of the State's Standard Operating System and personal productivity products (e.g. the current standard is Microsoft Windows XP for the operating system and Microsoft Office XP Professional for the personal productivity software, which means the median hardware configuration for Microsoft Windows 2000 and Microsoft Office 2000 Professional must be supported).

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will design and manage Workstation Equipment and Software configurations. The Offeror will also describe how it will document, implement, and maintain these configurations.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe the life cycle of their system(s) and the upgrade requirements as well as how it intends to remain current following full implementation.

The Offeror will provide an overview for how it will perform all functions required to perform Workstation Software distribution services, including installation planning, product installation, testing and certification.

The Offeror will provide an overview for how it will replace fixed function terminals and 3270 type devices to meet APA's business requirements.

The Offeror should describe how it will facilitate flexible, scalable Software distribution.

Describe the Offeror's approach for determining when to implement new releases of office automation software.

Describe your organizations proposed strategy for automated distribution of software to the desktop.

Describe your proposed strategy for implementing centrally managed backups of individual workstations.

Describe your organization's approach to providing ready-access documentation for all Authorized Users.

Local Area Network (LAN)

As of the Effective Date, Offeror will assume responsibility for the provision, deployment, operations, management and support of the State's LAN environment including the Equipment as described in Appendix E.

LAN support includes maintenance of the LAN environments including Servers, intelligent/non-intelligent hubs, switches, encryption/security devices, routing/bridging devices, various monitoring devices, and all other devices or technology encompassed within the LAN environments not under the direct control and authority of Authorized Users.

The Offeror will be responsible for establishing and maintaining connectivity for all desktops within the State's LAN including the ability for laptop devices to connect with the LANs.

In order to achieve the GTA's convergence objectives, the GTA desires the total integration of the LAN environment with the State's WAN and data centers in a manner that will preserve levels of security and reliability and does not compromise any element of the operation. Integration should include the extensive use of switching within the LAN to the Workstation, LAN backbone, and WAN.

The Offeror will be responsible for the upgrade of the existing LAN infrastructure. GTA desires an infrastructure capable of providing each Workstation with switched bandwidth; QoS capabilities; and VLAN segmentation. Individual Workstations or servers need to be provisioned with switched 100Mbps network access. Workstation wire capable of supporting 100Mbps access is required for each Workstation. Workstation wire not capable of supporting 100Mbps must be upgraded by the Offeror.

The Offeror may choose to deploy wireless solutions in order to meet the mobility desires of APAs. If so, the wireless solutions must be capable of meeting the GTA's convergence, security, QoS and committed information rate bandwidth objectives. The Offeror my also choose to deploy an integrated wired and wireless solution that offers Authorized Users wired connections that have higher bandwidth than wireless connections.

The GTA encourages the creative use of wireless solutions that meet the APA's needs.

The GTA desires that all LANs be connected to the WAN. GTA prefers the LAN access to the WAN to be via Transparent LAN Service to the greatest extent possible.

The Offeror will also be responsible for the deployment, operations and maintenance of specific Servers within the network. The Offeror is to achieve economies of scale by centralizing facilities where practical, and by consolidating hardware platforms where appropriate.

GTA desires the implementation of a single network system standard as selected by GTA. The Offeror will be responsible for the migration of existing servers to the State Standard Operating Systems.

The types of Servers that fall within the scope of this SOW include:

- File and print.
- APA domain controllers.
- Directory services servers.
- Exchange mailbox Server.
- Exchange public folder Server.
- SMTP Server.
- Exchange Front-end Server.
- Back-up/recovery Server.
- Tape library Server.
- Firewall Server.
- Proxy Server.
- Cache Server.
- Surrogate file Server.
- Gateway Server.
- Resource management Server (which is dedicated to the management of the previous Servers).
- Mobile Data Computing (MDC) Server

The following Servers do not fall within the scope of this SOW:

- Database Server.
- Application Server.
- Web Server.
- Resource management Server (which is dedicated to the management of the previous Servers).

Functional Requirements

The Offeror's solution should support:

Standardization on the use of dedicated LAN switching connections between LAN switch to Workstation connections; LAN switch to LAN switch connections; LAN switch to WAN connections; and WAN to WAN connection.

Deployment of uniform protocols within both the LAN and WAN.

Creation and implementation of statewide LAN hardware and configuration standards in conformance with GTA standards.

Upgrade of LAN hardware to meet GTA standards.

Upgrade of LAN wiring to meet GTA standards.

Maintenance and operations of all existing LAN and Server equipment until such a time as they are eliminated due to consolidation, the State's Standard Operating System upgrade, and/or refreshment.

Consolidation of Servers where appropriate and in accordance with Service Level objectives.

Deployment of the State's Standard Operating System for all Servers.

Backup of Servers in accordance to the Backup Service Level objectives; defined archival and data retention schedules; and Disaster Recovery operations.

Provide change management to ensure that planned modifications to the LANs conform to the requirements of a Change Control system and procedures.

Manage network performance and availability in accordance with the Service Levels. Continually monitor all systems, disks, queues, memory, CPU utilization, etc. to determine if the State's systems and LANs are operating properly. Modify system parameters to resolve application performance problems that manifest in system response times or other Service Levels. Take steps necessary to ensure that application perform at an optimal level; including adding hardware, or upgrading hardware, or upgrading hardware or the network infrastructure.

Maintain document of the LAN and Server physical and logical configurations. Provide GTA with access to electronic copies of the documentation.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

Describe your organization's approach for maintaining and operating the LAN and Server equipment located within State facilities.

Describe your organization's approach for to conducting Server consolidation and migration to a common network operating system.

Describe your organization's proposed LAN and Server architecture. Include descriptions of a typical LAN infrastructure for a small, medium, and large State facility. Include descriptions of both wired and wireless proposed solutions.

Describe how your proposed architecture supports increased mobility and MACs performed by Authorized Users (i.e., moving their own desktop device).

Describe your approach to upgrading and standardizing the LAN infrastructure to meet GTA standards

Describe your solution's ability to create and enforce security and convergence within the LAN. Specifically discuss both wired and wireless approaches if both are proposed.

Describe your organization's design criteria for deploying wireless technologies. Describe your organization's wireless designs.

Describe your organization's proposed strategy for establishing standards for logical elements of the State's LANs, such as; network addresses; sign-on names; server names and addresses; printer names; and other resource names. Describe the issues your organization would need to address in implementing the logical standards

How do you expect GTA to participate in the LAN and Server development/implementation projects?

Describe any new technologies, products, and capabilities that your organization proposes to implement that will improve GTA's ability to achieve convergence.

Describe your organization's approach to deploying new technologies and equipment refreshment over the life of the contract.

Describe the network elements or design components that support the Service Level objectives.

Describe your organization's proposed strategy for backing up LAN servers and storage devices. When does your organization plan to implement such a strategy?

Describe your organization's proposed solution for providing recovery of LAN systems and data. Describe how the LAN recovery plan integrates with the overall disaster recovery strategy.

Describe your organization's approach for establishing capacity thresholds (e.g., bandwidth utilization) that would trigger a process to review LAN resources for possible upgrade to support GTA's growth.

Describe your organization's experience in the deployment of Transparent LAN service; the integration of LANs and WANs; and the deployment of a uniform protocol.

Describe your organization's experience in the design, deployment, operation and maintenance of a convergent LAN infrastructure similar to that proposed to GTA.

Describe you organization's experience in the design, deployment, operation, and maintenance of a consolidated Server environment.

LAN Operations

LAN operations include the activities supporting and maintaining the LANs that are aimed at providing a high degree of services availability to the State.

Functional Requirements

The Offeror's solution should support:

Engineering, design and implementation of LANs using wired or wireless technologies that conform to established standards.

Updating and maintaining shared-use file Server libraries of the State's standard Software products.

Deployment of new LAN services as required to meet the State's business requirements in support of the Distributed Computing environment initiatives, remote computing, and Internet/Intranet access.

Work with the GTA to establish LAN standards that will meet performance expectations as defined in the Service Levels.

Installation, implementation, operation and maintenance of the State's Internet/Intranet connectivity and access systems for all devices connected to the State LANs, using technologically current tools, products, and methods.

Provisioning an automated tool that will identify the availability of a specific LAN Segment.

Implementing network segments/rings for Authorized User communities or Server emplacements, upgrades to the networking environment, or installations/upgrades to other synchronous and asynchronous network services.

Actions to grant or deny LAN access to Authorized Users in accordance with procedures developed and documented with the GTA's input and approval.

Providing operational support for data transmission (send/receive) consistent with commercial or GTA standards.

Creation and maintenance of printer queues and objects in accordance with GTA procedures and standards.

Provisioning printers as required to support the Authorized User population.

Responsibility for the management of the TCP/IP network address scheme for those areas under its direct control.

Implementing dynamic host configuration protocol (DHCP) and static IP addressing where appropriate.

Development of Server strategies and configurations for CPU, memory, disk and tape capacities for various Authorized User base levels (e.g., below 25 users, 25 - 50 users, 50 - 100 users, 100 - 250 users, 250 - 500 users, 500 - 1000 users, 1000 - 2000 users, and 2000 – 4000

users). Targeted Servers include all of those types of Servers that fall within the scope of this SOW

Perform all Move/Add/Change (MAC) services including the installation, relocation and change of all network/desktop devices, including peripherals. These activities will be performed at no additional cost.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will provide LAN operations services, which include installation and maintenance of LAN Equipment, operations of the State's Internet/Intranet connectivity, automation of LAN functions and support, and day-day operations management for the LAN environments.

Describe your organizations approach to providing connectivity for equipment owned by APA's that may or may not conform to the standard platform.

The Offeror will detail the ratio of Authorized Users to LAN resources, e.g. printers.

The Offeror will describe how it will provide logical design and connectivity for wired and wireless LANs for which it is responsible, including support of TCP/IP network addresses.

The Offeror will describe the extent of convergence included within the proposed LAN design. The Offeror will describe the methods by which QoS and CoS may be supported within the LAN.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

The Offeror will describe the life cycle of their system(s) and the upgrade requirements as well as how it intends to remain current following full implementation.

Directory Services/Account and Access Management

Access rights to specific software, devices and information are managed through user accounts that are assigned specified roles, granted and approved based on the user's function within the organization. Directory services can facilitate account and access management through hierarchical structures that store and organize objects and attributes that are extensible and scalable. The Offeror will be involved in the maintenance of the directories or sections of directories that support other functions that will not be supported by the Offeror.

Functional Requirements

APA's will retain authority for approval of all data and system access requirements for the systems that support their Authorized Users. The APA's will notify the Offeror about which Authorized Users are to be granted access to the Offeror-operated systems and the level of rights access to be granted.

GTA will authorize all changes to the directory tree structure.

The Offeror's solution should support:

For Authorized Users:

Responsibility for Authorized User account administration in accordance with the Procedures Manual.

Creating and publishing Authorized User request form(s) in electronic format that will enable Authorized Users to furnish the information for the creation or modification of network accounts and provide an electronic mechanism for approval for the action by a Designated User in the APA having authority to do so. The form(s) will allow Designated Users to request:

Proper access rights sufficient to provide the Authorized User with the necessary file system access.

System dial-up access.

A fixed IP address, with an explanation of the need for this.

Rights to execute applications.

Rights to receive software updates.

Enable the desktop to be managed by the vendor with a GTA approved monitoring and management methodology.

Creation, modification or deletion of an e-mail account.

Creating Authorized User accounts upon receipt of a properly completed request form that has been approved by a Designated User in the APA authorized to do so.

Suspending inactive user accounts.

Deleting user accounts.

Resetting user passwords according to GTA-required procedures.

Providing for automated or manual account synchronization with systems other than the LAN as required by the GTA. This is to be done in an organized manner within a proper approval mechanism. The Offeror should be prepared with a hierarchical approval mechanism should GTA desire such.

Executing periodic audits to identify accounts that should be removed, accounts with unusual access rights, poor passwords or unusual disk space requirements.

For groups:

Creation and maintenance of the minimum number of groups necessary to support the business needs of MPA's and VPA's as approved by the GTA.

Consolidation or deletion of groups when the need for such is no longer valid.

Granting Authorized Users membership only to the groups to which membership has been requested or where membership is automatically authorized in the Procedures Manual.

For organizational units:

Creation and maintenance of sufficient numbers of organizational units to define APAs, and major organizational divisions within such APAs, up to and including five levels from the root.

For domains:

Creating domains in accordance with the Procedures Manual.

Providing for backup domain controllers sufficient to satisfy the disaster recovery levels as described in the Procedures Manual.

For domain trees:

Refraining from any attempts to gain control over or access to the root of the domain tree.

Maintaining the domain trees as provided for by GTA.

Creating additional domain trees only with the expressed written consent of the GTA.

Maintaining replication sufficient to maintain performance and disaster resistance as prescribed in the Procedures Manual.

For domain forests:

Maintaining the domain forest as provided for by the GTA.

Creating additional domain forests only with the expressed written consent of the GTA.

Maintaining replication sufficient to maintain performance and disaster resistance as prescribed in the Procedures Manual.

For DNS:

Planning, documenting, implementing and administering that portion of DNS which is associated with directory services.

Providing for DNS replication as necessary for maintaining performance and a disaster resistant system.

For security:

Conducting periodic reviews to validate individual Authorized User access to resources is appropriate.

Recording all routine access transactions associated with Authorized Users authenticating to the directory structure as well as retaining this record for a period of no less than 60 days. Upon request, make these records available to Designated Users for purposes of conducting audits and internal investigations.

Information on failed attempts to access the directory structure as follows:

Recording all failed attempts and retaining the record of such attempts for a period of no less than 180 days.

Providing monthly reports to Designated Users.

Upon request, providing such records to Designated Users for purposes of conducting audits and internal investigations.

For file system:

Developing, implementing, and maintaining a set of automated and manual processes designed to enforce GTA's data access rules.

Provision of commercially available third party tools designed to prevent undeleting or recovering of files and data deleted by certain individuals as identified by GTA.

For application integration:

Participate in the planning for the integration of the vendor maintained directory with the GTA's enterprise directory initiative.

Provision Offeror maintained directory to allow for synchronization with GTA's enterprise directory structure.

Offeror's Solution Description

Will you meet the functional requirements detailed in the preceding section or do you have an alternative to meet the underlying business objectives? Y ___ N__

The Offeror will provide an overview for how it will administer each aspect of the Directory Services.

The Offeror will describe its experience in delivering these functions in environments similar to the State.

[Entire Section revised per Addendum 1]

SERVICE LEVELS AND SERVICE LEVEL PAYMENTS

INTRODUCTION

The following Service Level Payments (as defined below) have been designed to encourage the consistent and timely delivery of Service and value to GTA. Specifically, this section and the sections detailed below outline the circumstances under which the Offeror will be subject to (i) MASL Payments for failures in the performance of any MASLs, (ii) Missed Milestone Payments for failure to meet Critical Milestones and/or (iii) Extended Failure Assessments for extended failure to meet MASLs and/or Critical Milestones (all such payments detailed hereunder are collectively referred to as "Service Level Payments").

Each MASL has been created to identify key performance measures that will be used to evaluate the Offeror's delivery of the requested Services. Likewise, each Critical Milestone has been created to identify the key delivery dates for Offeror's delivery of the requested Services to which those Critical Milestones relate. (MASLs and Critical Milestones are hereinafter collectively referred to as "Service Levels"). The overriding goal in developing the Service Levels is to support GTA's desire to manage the Offeror by monitoring and measuring performance on GTA's most-important business requirements. Even with the development of Service Levels it is difficult and, at times, impossible, to ascertain the actual damages to GTA where the Offeror fails to meet a Service Level. Therefore, the payments for failure to meet Service Levels are intended to be mutually agreed, nonexclusive, liquidated damages that are the parties' estimate of the lost value to GTA for the failure to meet one or more of the Service Levels. The

goal of these liquidated damages is not to penalize the Offeror, but rather to provide a greater incentive to achieve the RFP's stated objectives and focus the Offeror on GTA's critical needs.

The GTA expects that MASLs will increase over time and that new MASLs may be added to reflect changing or new business requirements. Similarly, the GTA expects that new Critical Milestones may be added to reflect new business requirements or projects that are added after contract award. The GTA expects continuous improvement in Offeror's provision of Service and, therefore, expects to review MASLs at least yearly and, where appropriate, to adjust the MASLs upward to reflect such continuous improvement in Offeror's provision of Service. In addition, the Offeror should be prepared to negotiate new MASLs and MASL Payments (including Weighting Factor adjustments) to reflect changing or new business requirements. The Offeror's agreement to such changes shall not be unreasonably withheld. In no event will the Service Levels or the Service Level Payments set forth herein be reduced below the levels at which they are set on the Signing Date.

At-Risk Amount

"At-Risk Amount" means eighteen percent (18%) of the Annual Services Charge where the Measurement Interval for Service Levels is annual; or eighteen percent (18%) of one-twelfth ($1/12^{th}$) of the Annual Services Charge where the Measurement Interval for Service Levels is monthly. With respect to the Critical Milestones, the "At-Risk Amount" is one-twelfth ($1/12^{th}$) of the Annual Services Charge for the applicable Contract Year.

MASL Payments and Missed Milestone Payments may exceed the At-Risk Amount for any Measurement Interval less than one year; however, the sum of all MASL Payments and Missed Milestone Payments for any Contract Year may never exceed the total At-Risk Amount for that Contract Year. Notwithstanding the foregoing, Service Level Payments are not the exclusive remedy to GTA for failures to meet the Service Levels or any other terms or conditions of the award.

Missed Milestone FAILURE DATE AND missed milestone FAILURE INTERVAL for Critical Milestones

"Missed Milestone Failure Date" means the date on which the Offeror has failed to meet its performance obligations in respect of a given Critical Milestone by the end of the Completion Period. The Missed Milestone Failure Interval means the period during which a given Critical Milestone failure continues (e.g., one day, one month, one year, etc.), and shall be as set forth in the Missed Milestone Failure Interval column in Schedule A.1 for a given Critical Milestone. After a failure to meet a Critical Milestone, the number of Missed Milestone Failure Intervals shall be determined by counting the number of Failure Intervals (a partial Failure Interval shall be counted as one) between the Failure Date and the ultimate completion date for such Critical Milestone.

Measurement Interval for MASLS

"Measurement Interval" means the period in which a given MASL is measured (e.g., one month, one year, etc.). The Measurement Interval for each MASL shall commence on the SLA Compliance Date set forth in Schedule A.1.

Weighting Factor

"Weighting Factor" means, for any MASL, or Critical Milestone, the factor that is applied to the At-Risk Amount for purposes of calculating the applicable Service Level

Payments in the event of any Failure. The Weighting Factor for each MASL and each Critical Milestone is set forth in Schedule A.1. The total of the Weighting Factors (i) for Contract Year 1 is one hundred percent (100%); (ii) for each of Contract Years 2-4, shall not exceed one hundred twenty percent (120%), and (iii) for each of the Contract Years 5-10, there shall be a five percent (5%) increase above the previous Contract Year Weighting Factor. In no event will the Weighting Factors set forth herein be reduced below the levels at which they are set on the Signing Date.

MASL Payments

MASL Payments

Initial Failure

In the event of any Failure with respect to a MASL, a MASL Payment will be imposed on Offeror; such MASL Payment shall be equal to the product of: (i) the At-Risk Amount, multiplied by (ii) the Weighting Factor for the MASL that was missed.

Subsequent Failures

If there are Failures as to a single Service Level in two or more consecutive Measurement Intervals, the Weighting Factor for the second, third, and subsequent consecutive Measurement Intervals shall be increased as follows:

Second Measurement Interval:	2 x the Weighting Factor
Third Measurement Interval:	4 x the Weighting Factor
Subsequent Measurement Intervals:	4 x the Weighting Factor

MASL Payment Reductions

If there are Failures as to a single Service Level in two or more consecutive Measurement Intervals, Offeror may earn a MASL Payment Reduction equal to fifty percent (50%) of the MASL Payment for the last Measurement Interval immediately preceding the Failure corresponding to a particular MASL if, in four (4) consecutive Measurement Intervals immediately following correction of the Failure, no Failure occurs as to that MASL; provided that if the MASL is measured annually, Offeror may earn a MASL Payment Reduction if no Failure occurs as to that MASL in such annual Measurement Interval.

Missed Milestones Payments

In the event of any Failure with respect to a Critical Milestone, a Missed Milestone Payment will be imposed on Offeror. Such Missed Milestone Payment shall be equal to the product of: (i) the At-Risk Amount, multiplied by (ii) the Weighting Factor for the Critical Milestone that was missed. Offeror shall be subject to a Missed Milestone Payment in the event the Offeror fails to meet a Critical Milestone by the end of the Completion Period and such Missed Milestone Payment shall be assessed once on the Missed Milestone Failure Date, and once again for each Missed Milestone Failure Interval after the Missed Milestone Failure Date during which the Critical Milestone failure continues.

MASL Payment ANNUAL CAP

The total amount of MASL Payments and Missed Milestone Payments for all Failures related to Service Levels in a single month may exceed eighteen percent (18%) of one-twelfth ($1/12^{th}$) of the Annual Services Charge for the applicable Contract Year.

However, the total amount of MASL Payments and Missed Milestone Payments for all such Failures related to Service Level (excluding Extended Failure Assessments) may not cumulatively exceed the total At-Risk Amount for any given Contract Year; provided that Service Level Payments are not the exclusive remedy to GTA for failures to meet the Service Levels or any other terms or conditions of the award.

EXTENDED FAILURE ASSESSMENTS

Although the sum of all MASL Payments and Missed Milestone Payments may not exceed the total At-Risk Amount for the applicable Contract Year, additional "Extended Failure Assessments" may be applied for extended failures to meet Service Levels. Extended Failure Assessments are intended to be mutually agreed, nonexclusive, liquidated damages that are the parties' estimate of the additional lost value to GTA for extended failures to meet Service Levels. Any amounts levied as Extended Failure Assessments are not limited to the At-Risk Amount defined in the previous sections; are due in addition to any MASL or Missed Milestone Payments; and are nonexclusive remedies. There shall be no ceiling on Extended Failure Assessments. Extended Failure Assessments are also not subject to MASL Payment Reduction provisions.

Extended FAILURE DATE AND THE Extended Failure Interval for SERVICE LEVELS

"Extended Failure Date" means the date on which the Offeror has failed to meet its performance obligations in respect of a given Service Level by the end of the Extended Failure Interval. The Extended Failure Interval means an extended period during which a given Service Level Failure continues (e.g., one day, one month, one year, etc.), as set forth in the Extended Failure Interval column in Schedule A.1 for a given Service

Level. After a Failure to meet a Service Level that continues for the Extended Failure Interval, an Extended Failure Assessment shall be assessed for that extended failure on the Extended Failure Date. Thereafter, additional Extended Failure Assessments shall be assessed for that extended failure as determined by counting the number of Extended Failure Intervals (a partial Failure Interval shall be counted as one) between the Extended Failure Date and the ultimate date of satisfaction or completion for such Critical Milestone.

PAYMENT OF SERVICE LEVEL PAYMENTS

All Service Level Payments for all Failures shall be made on a monthly basis to GTA as steward for the State. Where the Measurement Interval is less than one month, the Service Level Payments will be aggregated and billed monthly. Where the Measurement Interval is greater than one month, the Service Level Payments will be paid on the month immediately following the Failure.

GEORGIA TECHNOLOGY AUTHORITY

Schedule A.1 Minimum Acceptable Service Levels

Contract Year 1

Minimum Acceptable Service Levels	% of Weighting Factor	Extended Failure Assessment (MASL Monthly at Risk Amount)	Extended Failure Interval	SLA Compliance Date
Data Communications				
GoNetGo Network Service	13%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Access Line Service	13%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Video Communications - Service	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Voice Communications – Service	21%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Statewide 911				
911 System Availability	4%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Emergency Device Call Completion	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Cross Functional				
Help Desk Support	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Help Desk Problem Response	8%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Help Desk IMACs	4%	Sum of the previous 4	Every 4th	Cutover

Minimum Acceptable Service Levels	% of Weighting Factor	Extended Failure Assessment (MASL Monthly at Risk Amount)	Extended Failure Interval	SLA Compliance Date
		consecutive MASL payments	Subsequent Interval Failure	Date
Customer Satisfaction	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Distributed Computing – Service	5%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
2-Way Radio & Mobile Digital Communications	11%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
AVL	0%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
Mobile Data & Messaging	5%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
TV/Radio Broadcast and Distribution	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date
GDOT Navigator	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Cutover Date

Schedule A.2: Critical Milestones

Contract Year 1

Critical Milestones	Weighting Factor	Completion Period	Missed Milestone Failure Interval	Extended Failure Assessment	Extended Failure Interval
Employee Transition	2.5%	**May 1, 2003**	Monthly	$650,000.00	Monthly
Transition Plan documented, approved and executable.	**5%**	**February 15, 2003**	**Monthly**	**N/A**	**N/A**
Transformation Plan documented, approved and executable.	**5%**	**April 1, 2003**	**Monthly**	**N/A**	**N/A**
Order fulfillment process in operation as defined in SOW.	10%	Cutover Date	Monthly	N/A	N/A
Helpdesk implemented as defined in the SOW.	10%	Cutover Date	Monthly	N/A	N/A
Change Mgmt. Process developed, approved and implemented as defined in SOW.	5%	Cutover Date	Monthly	N/A	N/A
Problem Mgmt. Process developed, approved and implemented as defined in SOW.	5%	Cutover Date	Monthly	N/A	N/A
Service Monitoring operating as defined in the SOW.	5%	Cutover Date	Monthly	N/A	N/A
Billing System operating as defined in the SOW.	7.5%	Cutover Date	Monthly	N/A	NA
SLA Reporting as defined in the SOW and Service Levels.	5%	30 days from Cutover Date	Monthly	$25,000.00	Every 3rd Subsequent Interval Failure
Operational Procedure manual developed and approved as defined in the SOW.	2.5%	90 days from Cutover Date.	Monthly	N/A	N/A
Quick Response plan developed, approved and documented as defined in the SOW.	5%	90 days from Cutover Date.	Monthly	$2,000,000.00	Annually

Critical Milestones	Weighting Factor	Completion Period	Missed Milestone Failure Interval	Extended Failure Assessment	Extended Failure Interval
Disaster Resistance Plan developed and submitted for approval and implemented as defined in the SOW.	7.5%	90 days from Cutover Date.	Monthly	$1,000,000.00	Annually
Satisfaction Survey's developed using survey content created by GTA.	5%	90 days from Cutover Date.	Monthly	N/A	N/A
Implementation of an Information Security program for safeguarding the State's information as defined in the SOW.	10%	120 days from Cutover Date.	Monthly	N/A	Every 3rd Subsequent Interval Failure
Quality Assurance process developed, approved and implemented as defined in the SOW.	2.5%	180 days from Cutover Date.	Monthly	N/A	N/A
Performance, capacity and configuration plan developed, approved and implemented as stated in the SOW.	2.5%	180 days from Cutover Date.	Monthly	N/A	N/A
GPB-Digital TV	**0%**	**Begin at Effective Date**	**Monthly**	**N/A**	**N/A**
GPB-Digital TV Completion	**5%**	Installed no later than 05/31/03.	Monthly	Assume liability for any penalties assessed against the State	Monthly
Two Way Radio Infrastructure	**0%**	**Begin at Effective Date**	**Monthly**	**N/A**	**N/A**
Subtotal of Critical Milestones:	100%				
(% of At Risk Amount):	30%				
Total Service Level and Critical Milestone Weighting- Contract Year 1					

Schedule A.3: Minimum Acceptable Service Levels

Contract Year 2 through Term

Minimum Acceptable Service Levels	% of Weighting Factor	Extended Failure Assessment	Extended Failure Interval	SLA Compliance Date
Data Communications				
GoNetGo Network Service	19%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Access Line Service	5%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Lambda Transport Service	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Video Communications - Service	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Voice Communications – Service	21%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Statewide 911				
911 System Availability	4%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Emergency Device Call Completion	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Cross Functional				
Help Desk Support	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Help Desk Problem Response	8%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Help Desk IMACs	4%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Customer Satisfaction	3%	N/A	N/A	Beginning of 13th Month
Distributed Computing – Service	3%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month

Minimum Acceptable Service Levels	% of Weighting Factor	Extended Failure Assessment	Extended Failure Interval	SLA Compliance Date
2-Way Radio & Mobile Digital Communications	11%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
AVL	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
Mobile Data & Messaging	5%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
TV/Radio Broadcast and Distribution	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month
GDOT Navigator	2%	Sum of the previous 4 consecutive MASL payments	Every 4th Subsequent Interval Failure	Beginning of 13th Month

Schedule A.4: Critical Milestones

Contract Year 2

Critical Milestones	Weighting Factor	Completion Period	Missed Milestone Failure Interval	Extended Failure Assessment	Extended Failure Interval
1. Two-Way Radio deployment to meet availability and coverage Service Levels.	15%	Deployed 18 months from Cutover Date	Monthly	$1,000,000.00	Every 3rd Subsequent Interval Failure
2. Deployment of Standard workstation Software as defined in the SOW.	15%	24 months from Cutover Date	Monthly	$250,000.00	Every 3rd Subsequent Interval Failure
3. Asset Management repository populated with hardware and software configuration data for all electronically discoverable configurations.	10%	365 days from Cutover Date.	Monthly	$250,000.00	Every 3rd Subsequent Interval Failure
4. State Wide Wireless service.	10%	365 days from Cutover Date.	Monthly	$500,000.00	Every 3rd Subsequent Interval Failure
5. AVL deployment	10%	365 days from Cutover Date.	Monthly	$250,000.00	Every 3rd Subsequent Interval Failure
Total Weighting Factor (% of At Risk Amount):	20%				
Total Service Level and Critical Milestone Weighting – Contract Year 2					

Schedule A5: Critical Milestones

Contract Year 3 through term

Critical Milestones	Weighting Factor	Completion Period	Missed Milestone Failure Interval	Extended Failure Assessment	Extended Failure Interval
1. Data Network as	20%	30 months from	Monthly	$500,000.00	Every 3rd

Critical Milestones	Weighting Factor	Completion Period	Missed Milestone Failure Interval	Extended Failure Assessment	Extended Failure Interval
defined in SOW.		Cutover Date			Subsequent Interval Failure
2. All Transformation Complete.	20%	30 months from Cutover Date	Monthly	$500,000.00	Every 3rd Subsequent Interval Failure
Total Weighting Factor (% of At Risk Amount):	10%				
Total Service Level and Critical Milestone Weighting – Contract Year 3					

End of Schedule